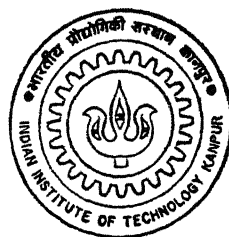


# ON CERTAIN COMPUTATIONS RELATED TO ELLIPTIC CURVES

by

K. P. P. Kalyan Chakravarthy



DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

FEBRUARY, 1996

TH  
EE/1996/14  
C 3490

EE

1996

M

CHA

CER

# **ON CERTAIN COMPUTATIONS RELATED TO ELLIPTIC CURVES**

*A Thesis Submitted*  
in Partial Fulfillment of the Requirements  
for the Degree of  
**Master of Technology**

*by*  
**K.P.P. Kalyan Chakravarthy**

*to the*  
**DEPARTMENT OF ELECTRICAL ENGINEERING  
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR**

**February 1996**

21 MAR 1996  
CENTRAL LIBRARY  
I. I. T. KANPUR  
121204

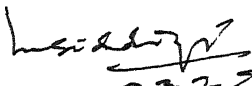
EE-1996-M-CHA-ON



A121204

# CERTIFICATE

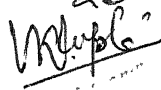
This is to certify that Mr K.P.P. Kalyan Chakravarthy, Roll No 9410423 has carried out the thesis work titled "ON CERTAIN COMPUTATIONS RELATED TO ELLIPTIC CURVES " under my supervision and the same is not submitted elsewhere for a degree.

  
23.2.96

Dr. M. U. Siddiqi

Prof. Dept. of EE.

(Thesis Supervisor)

23.2.96  
  
K.P.P. Kalyan Chakravarthy



# ABSTRACT

Computations related to elliptic curves over finite fields have in recent years gained much attention not only because elliptic curves over finite fields are a rich source of abelian groups which can be used to implement public key cryptosystems but also because they have stimulated a new direction of research in computational number theory. Common to all the computational problems is the design of suitable elliptic curves e.g. primality proving. For the implementation of elliptic curve cryptosystems, we need to construct nonsupersingular curves which have the given large group order over large finite fields. The finite fields which are of practical interest are the prime fields and those extensions of  $\text{GF}(2)$  which have an optimal normal basis in them. In this thesis, we will see the computations involved in the design of such suitable curves and those related to the implementation of cryptosystems using those curves.

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>The Review of Arithmetic Of Elliptic Curves</b>	<b>4</b>
2.1	Curves Over $\mathbb{C}$ . . . . .	4
2.2	Curves Over Local Fields . . . . .	8
2.3	Complex Multiplication . . . . .	15
2.4	Class Field Theory : A Brief Review . . . . .	17
2.5	Class Invariants . . . . .	19
2.6	Weber's Class Invariants: . . . . .	21
<b>3</b>	<b>Optimal Normal Basis</b>	<b>23</b>
3.1	Optimality Criterion . . . . .	23
3.2	Construction of Optimal Normal Bases . . . . .	25
3.3	Explicit construction of Type II ONBGs . . . . .	25
3.4	Matrix of Transformation 'T' . . . . .	26
<b>4</b>	<b>Gao and Vanstone Basis</b>	<b>30</b>
4.1	A New Basis . . . . .	30
4.2	Bilinear Form Derived . . . . .	33
<b>5</b>	<b>Design and Implementation</b>	<b>35</b>
5.1	Certain Computations . . . . .	35
5.2	Construction of Elliptic Curves . . . . .	41
5.3	Solving the Norm Equation . . . . .	52
<b>6</b>	<b>Results and Conclusion</b>	<b>54</b>
6.1	Normal Basis Arithmetic . . . . .	54
6.2	Elliptic Curve Cryptosystems . . . . .	55
6.3	Design of Elliptic Curves . . . . .	56
6.4	Conclusions . . . . .	62

## Chapter 1

# Introduction

The invention of public key cryptography by Diffie and Hellman in 1976 not only revolutionized the field of cryptography, but also had a profound effect on the direction of research in computational number theory. For the first time the question of the relative complexity of various number-theoretic tasks took on a practical urgency.

The first usable public key system, introduced in 1978, was the RSA cryptosystem, which is based on the problem of factoring large integers. RSA soon became the best known and most widely used public key cryptosystem. It stimulated a tremendous amount of research on the twin subjects of factoring and primality testing.

Another type of public key cryptography — based the discrete analogue of the logarithm function — gave rise to a second current of research in computational number theory. The discrete log problem was first considered in the multiplicative group of a finite field, especially a prime finite field or a finite field of characteristic of 2 (since these fields seemed to be the most practical for implementation). Although discrete log cryptosystems have been in the public eye much less than RSA, the discrete log problem and related issues have been receiving considerable attention in the research community. The practical questions that have arisen in discrete log cryptography have served as an impetus for much work on the structure of finite fields and the complexity of certain tasks related to this structure.

In 1985 a variant of discrete log cryptography was proposed, based on the discrete log problem in the group of points of an elliptic curve defined over a finite field. Cryptosystems using discrete logarithms in this group have two potential advantages over systems based on the multiplicative group of a finite field (and also over systems based on RSA): (1) the great diversity of elliptic curves available to provide the groups; and (2) the absence of subexponential time algorithms (such as those of ‘index calculus’ type) that could find discrete logs in these groups [Men1].

Of the developments in elliptic curve cryptography since 1985, the most dramatic was the demonstration by Menezes, Okamoto and Vanstone in 1990 that the discrete log problem on a so called ‘supersingular’ elliptic curve can be reduced to (i.e., has the same complexity as) the discrete log problem in a finite field. This result means that one should avoid the (relatively small) set of supersingular curves if one wants to have a cryptosystem whose cracking problem is, to the best of our current knowledge, of fully exponential complexity.

Clearly, if devising efficient algorithms for the blocks involved in the implementation of any scheme of elliptic curve cryptosystems is one important aspect of research, developing an efficient algorithmic procedure for the design of curves suitable for use in these systems is also an important aspect of it. Atkin and Morain first brought out an algorithmic procedure, as a by product of their implementation of the so called ‘Elliptic Curve Primality Proving’ method proposed by Lenstra [Kob1]. Their method uses Class Field Theory and Weber’s Class Invariants. Lay and Zimmer also developed a similar procedure which is almost same as that of Atkin and Morain but differs in the chosen Class Invariants and the way Class Equations (minimal polynomials of the suitably chosen Class Invariants of the Ring Class Field of concern) are computed. They have also developed a procedure to design curves over  $\mathbb{F}_{2^n}$  using the Yui-Zagier Reduced Class Equation.

In this thesis, we will see the algorithmic procedure of Lay and Zimmer and the implementation of it using the arithmetic packages SIMATH/simcalc and PARI/GP. We will also look into all the computations involved in the implementation of elliptic curve cryptosystems and how to do them efficiently using the currently known best algorithms. Apart from this, we will also look into certain computations related to normal basis arithmetic, which will be needed by us.

The organization of the thesis is as follows: We will first review the arithmetic of elliptic curves in Chapter 2. In Chapters 3 and 4, we will see certain aspects related to optimal normal basis. Chapter 5 is concerned with the computations involved in the design and implementation of elliptic curve cryptosystems. As said above, we will be concerned with only the currently known most efficient algorithms. In Chapter 6, we list the results of our implementation of all the algorithms discussed in the previous chapters.

## Chapter 2

# The Review of Arithmetic Of Elliptic Curves

In this chapter let us look into the main results which help us in understanding the theory of elliptic curves from computational point of view. That is we will see those results which will lead us to understanding of the problem of building an elliptic curve of given group order over large finite fields which we will see in the Chapter 5.

## 2.1 Curves Over $\mathbb{C}$

Let us consider some of the definitions related to the theory of elliptic curves [Silv1] (for the basic theory of elliptic curves [Chah] [Rose] [More]). Let  $E(\mathbb{C})$  be an elliptic curve defined over  $\mathbb{C}$  and  $P$  any point on the curve. (It is assumed that  $\mathcal{O}$  is the point at infinity) We start with the hypothetical map  $E(\mathbb{C}) \rightarrow \mathbb{C}$  defined by:

$$P \rightarrow \int_{\mathcal{O}}^P \omega = I$$

and the two integrals,

$$\omega_1 = \int_{\alpha} \omega \text{ and } \omega_2 = \int_{\beta} \omega$$

which are called periods of  $E$ , which allow us to visualize how elliptic curves have evolved out naturally out of the so called *elliptic integrals* [Alf] [Silv1]. We find that the integral  $I$  given above is well-defined upto addition of a number of the form  $n_1\omega_1 + n_2\omega_2$ . Let

$$\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$$

We have thus

$$F : E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda$$

$$P \rightarrow \int_0^P \omega \pmod{\Lambda}$$

Using the translation invariance of  $\omega$ , we can easily verify that  $F$  is a homomorphism. (The group law on  $\mathbb{C}/\Lambda$  being induced by addition on  $\mathbb{C}$ . Now the quotient space  $\mathbb{C}/\Lambda$  will be a Riemann surface (i.e. a one dimensional complex manifold  $\Rightarrow$  complex torus). iff  $\Lambda$  is a lattice; that is iff the periods  $\omega_1$  and  $\omega_2$  which generate  $\Lambda$  are linearly independent over  $\mathbb{R}$  [Silv1]. This is the case and  $F$  gives a complex analytic isomorphism. Let us now study the space  $\mathbb{C}/\Lambda$  for a given lattice  $\Lambda$  by constructing the inverse to the mapping  $F$ , and show that  $\mathbb{C}/\Lambda$  is analytically isomorphic to  $E_\Lambda(\mathbb{C})$  for a certain elliptic curve  $E_\Lambda/\mathbb{C}$ . The *Uniformization Theorem* then says that every elliptic curve (e.c)  $E/\mathbb{C}$  is isomorphic to some  $E_\Lambda$ , from which we will see that the periods of  $E/\mathbb{C}$  are  $\mathbb{R}$ -linearly independent and that  $F$  is a complex analytic isomorphism.

Let  $\Lambda \subset \mathbb{C}$  be a lattice, that is,  $\Lambda$  is a discrete subgroup of  $\mathbb{C}$  which contains an  $\mathbb{R}$ -basis for  $\mathbb{C}$ . Now let us see meromorphic functions [Alf] on the quotient space  $\mathbb{C}/\Lambda$ ; or equivalently, meromorphic functions on  $\mathbb{C}$  which are periodic with respect to the lattice  $\Lambda$ .

**Def 1:** An *elliptic function* (relative to the lattice  $\Lambda$ ) is a meromorphic function  $f(z)$  on  $\mathbb{C}$  which satisfies

$$f(z + \omega) = f(z) \quad \forall \omega \in \Lambda, z \in \mathbb{C}$$

The set of all such functions is denoted  $\mathbb{C}(\Lambda)$ .  $\mathbb{C}(\Lambda)$  is clearly a field [Alf].

The Weierstrass  $\wp$ -function (relative to  $\Lambda$ ) is defined by the series

$$\wp(z, \Lambda) = 1/z^2 + \sum_{\omega \in \Lambda, \omega \neq 0} 1/(z - \omega)^2 - 1/\omega^2$$

We have

$$\mathbb{C} = \mathbb{C}(\wp(z), \wp'(z))$$

That is, every elliptic function is a rational combination of  $\wp$  and  $\wp'$ .

The Laurent series for  $\wp$  about  $z = 0$  is given by

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z_{2k},$$

for all  $z \in \mathbb{C}$  with  $z \notin \Lambda$ ,

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$$

where

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-2k}$$

is the Eisenstien series of weight  $2k$ (for  $\Lambda$ ) . It is standard notation to set

$$g_2 = g_2(\Lambda) = 60G_4 \text{ and}$$

$$g_3 = g_3(\Lambda) = 140G_6.$$

Then the algebraic relation between  $\wp(z)$  and  $\wp'(z)$  reads

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Let  $E/\mathbb{C}$  be an elliptic curve. Since the group law  $E \times E \rightarrow E$  is given by everywhere locally defined functions, we see in particular that  $E = E(\mathbb{C})$  is a complex Lie group(i.e a complex manifold with a group law given locally by complex analytic functions). Similarly if  $\Lambda \subset \mathbb{C}$  is a lattice, then  $\mathbb{C}/\Lambda$  with its natural addition is a complex Lie group. The next proposition shows that  $\mathbb{C}/\Lambda$  is always complex analytically isomorphic to an elliptic curve.

**Prop 1:** Let  $g_2$  and  $g_3$  be the quantities associated to a lattice  $\Lambda \subset \mathbb{C}$ .

(a)The polynomial  $f(x) = 4x^3 - g_2x - g_3$  has distinct roots. Its discriminant:

$$\Delta(\Lambda) = g_2^3 - 27g_3^2$$

is not zero. (b)Let  $E/\mathbb{C}$  be the curve:

$$E : y^2 = 4x^3 - g_2x - g_3,$$

which is an elliptic curve from (a). Then the map

$$\begin{aligned} \phi & : \mathbb{C}/\Lambda \rightarrow E \subset \mathbb{P}^1(\mathbb{C}) \\ & : z \rightarrow [\wp(z), \wp'(z), 1] \end{aligned}$$

is a complex analytic isomorphism of complex Lie groups (that is it is an isomorphism of Riemann Surfaces which is a group homomorphism).

Let  $\Lambda_1$  and  $\Lambda_2$  be two lattices in  $\mathbb{C}$ .If  $\alpha \in \mathbb{C}$  has the property that  $\alpha\Lambda_1 \subset \Lambda_2$ , then the scalar multiplication by  $\alpha$ :

$$\begin{aligned} \phi & : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2 \\ \phi_\alpha(z) & = \alpha z \bmod \Lambda_2 \end{aligned}$$

is clearly a holomorphic homomorphism. The important fact is that these are essentially the only holomorphic maps. We have thus the following important theorem which lead to some useful conclusions:

**Theorem 1:**(a)With the notation as above, the association:

$$\begin{aligned} \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} &\rightarrow \\ \{\text{holomorphic maps } \phi : \mathbb{C}/\Lambda &\rightarrow \mathbb{C}/\Lambda \text{ with } \phi(0) = 0\} \\ \alpha &\rightarrow \phi_\alpha \text{ is a bijection} \end{aligned}$$

(b)Let  $E_1$  and  $E_2$  be the elliptic curves corresponding to the lattices  $\Lambda_1$  and  $\Lambda_2$  as in the above proposition. Then the natural inclusion:

$$\begin{aligned} \{\text{isogenies } \phi : E_1 &\rightarrow E_2\} \rightarrow \\ \{\text{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 &\rightarrow \mathbb{C}/\Lambda_2 \text{ with } \phi(0) = 0\} \end{aligned}$$

is a bijection.

An Immediate corollary follows:

**Corr 1:**Let  $E_1/\mathbb{C}$  and  $E_2/\mathbb{C}$  be elliptic curves corresponding to lattices  $\Lambda_1$  and  $\Lambda_2$  as in the above proposition Then  $E_1$  and  $E_2$  are isomorphic (over  $\mathbb{C}$ ) iff  $\Lambda_1$  and  $\Lambda_2$  are homothetic (i.e  $\Lambda_1 = \alpha\Lambda_2$  for some  $\alpha \in \mathbb{C}$ ).

Now we reach the Uniformization Theorem for elliptic curves which says that every elliptic curve over  $\mathbb{C}$  is parametrized by elliptic functions. The most natural proof of this fact uses the theory of *modular functions*: that is functions on the set of lattices of  $\mathbb{C}$ . (For example  $g_2$  and  $g_3$  are modular functions)

**Uniformization Theorem** :Let  $A, B \in \mathbb{C}$  satisfy  $A^3 - 27B^2 \neq 0$ . then there exists a unique lattice  $\Lambda_1 \subset \mathbb{C}$  such that  $g_2(\Lambda) = A$  and  $g_3(\Lambda) = B$ .

**Corr 2:**Let  $E/\mathbb{C}$  be an elliptic curve. Then there exists a lattice  $\Lambda \subset \mathbb{C}$ , unique upto homothety, and a complex analytical isomorphism:

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\rightarrow E(\mathbb{C}) \\ \phi(z) &= (\wp(z, \Lambda), \wp'(z, \Lambda)) \end{aligned}$$

of complex Lie groups.

Much of the preceding material can be summarized as an equivalence of categories [Lang1]:

The following categories are equivalent :

(a)**Objects:**Elliptic curves over  $\mathbb{C}$ ,

**Maps:**Isogenies.

(b)**Objects:**Elliptic curves over  $\mathbb{C}$ .



**Maps:**Complex analytical maps taking  $\mathcal{O}$  to  $\mathcal{O}$ .  
(c)**Objects:**Lattices  $\Lambda \subset \mathbb{C}$ , upto homothety,  
**Maps:** $\text{Map}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$ .

The previous theorem is important in that it allows us to identify  $\text{End}(E)$  of  $E/\mathbb{C}$  with a certain subring of  $\mathbb{C}$ . Thus if  $E/\mathbb{C} \cong \mathbb{C}/\Lambda$  as in the previous corollary. then

$$\text{End}(E) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$$

Since  $\Lambda$  is unique upto homothety(Corr 1) , this ring is independent of  $\Lambda$ . We now use this description of  $\text{End}(E)$  to completely characterize the possible endomorphism rings which can occur. We recall the following definition:

**Def :**Let  $K$  be a number field. An *order*  $\mathcal{O}$  of  $K$  is a subring of  $K$  which is finitely generated as a  $\mathbb{Z}$ -module and satisfies  $\mathcal{O} \otimes \mathbb{Q} = K$ .

Now we have the most important theorem in the sense that it is the starting point . apart from the results in Class Field Theory which we need.

**Theorem 2:**Let  $E/\mathbb{C}$  be an elliptic curve and let  $\omega_1, \omega_2$  be generators for the lattice  $\Lambda$  associated to  $E$  by Corr 2. Then either :

- (i)  $\text{End}(E) = \mathbb{Z}$  or
- (ii)  $\mathbb{Q}(\omega_1/\omega_2)$  is a imaginary quadratic extension of  $\mathbb{Q}$ , and  $\text{End}(E)$  is isomorphic to an order in  $\mathbb{Q}(\omega_1/\omega_2)$ .

As a consequence if the above results , we have the following property of curves over fields of characteristic 0:

Let  $K$  be a field of char=0 and  $E/K$  an elliptic curves.

- (a) Let  $m \geq 1$  be an integer. Then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

- (b) The endomorphism ring of  $E$  is either  $\mathbb{Z}$  or an order in a imaginary quadratic extension of  $\mathbb{Q}$ . Now let us see some of the properties of elliptic curves defined over a local fields and hence look into the results available in the study of group of rational points on an e.c defined over a field which is complete w.r.t a discrete valuation, in the following section[Chah] [Lang2] [Shaf2] [Lang1].

## 2.2 Curves Over Local Fields

Before looking into the main results, let us look into the notation used in the sequel:

$K$ : a local field, complete w.r.t a discrete valuation  $v$  [Lang1] [Chah].

$\mathcal{O}_K$ : The ring of integers of  $K = \{x \in K : v(x) \geq 0\}$

$\mathcal{O}_K^*$ : The unit group of  $\mathcal{O}_K = \{x \in K : v(x) = 0\}$

$M$ : The maximal ideal of  $\mathcal{O}_K \Rightarrow \{x \in K : v(x) > 0\}$

$\pi$ : A uniformizer for  $\mathcal{O}_K$  (i.e  $M = \pi\mathcal{O}_K$ )

$k$ : The residue field of  $\mathcal{O}_K = \mathcal{O}_K/M$ .

We further assume that  $v$  is normalized so that  $v(\pi) = 1$  and both  $K$  and  $k$  are perfect fields [Lang1] [Chah].

**Def**: Let  $E/K$  be an elliptic curve. A Weierstrass equation is called a *minimal Weierstrass equation* for  $E$  at  $v$  if  $v(\Delta)$  is minimized subject to the condition  $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_K$ . This value of  $v(\Delta)$  is the *valuation of the minimal discriminant of  $E$  at  $v$* .

We have the following proposition:

**Prop 3.** (a) Every elliptic curve  $E/K$  has a minimal Weierstrass equation .  
(b) A minimal Weierstrass equation is unique upto a change of coordinates:

$$x = u^2x' + r; y = u^3y' + u^2sx' + t$$

with  $u \in \mathcal{O}_K^*$  and  $r, s, t \in \mathcal{O}_K$ .

(c) Conversely if one starts with any Weierstrass equation with coefficients  $a_i \in \mathcal{O}_K$ , then any change of coordinates:

$$x = u^2x' + r; y = u^3y' + u^2sx' + t$$

used to produce a minimal Weierstrass equation satisfies  $u, s, t, r \in \mathcal{O}_K$ .

**Reduction modulo  $\pi$** : We next look at the operation of *reduction modulo  $\pi$*  which we denote by a tilde. Thus, for example, the natural reduction map  $\mathcal{O}_K \rightarrow k = \mathcal{O}_K/M$  is denoted  $t \rightarrow \tilde{t}$ . Now having chosen a minimal Weierstrass equation for  $E/K$ , we can reduce its coefficients modulo  $\pi$  to obtain a (possibly singular) curve over  $k$  namely:

$$\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_4x + \tilde{a}_6$$

The curve  $\tilde{E}/k$  is called reduction of  $E$  modulo  $\pi$ . From the above proposition, since we started with a minimal equation for  $E$ , the equation  $\tilde{E}$  is unique upto the standard change of coordinates for Weierstrass equations over  $k$ .

Next let  $P \in E(K)$ . We can find homogeneous coordinates  $P = [x_0, y_0, z_0]$  with  $x_0, y_0, z_0 \in \mathcal{O}_K^*$ . Then the reduced point  $\tilde{P} = [\tilde{x}_0, \tilde{y}_0, \tilde{z}_0]$  is in  $\tilde{E}(K)$ . This gives the *reduction map*.

$$\begin{aligned} E(K) &\rightarrow \tilde{E}(K) \\ P &\rightarrow \tilde{P} \end{aligned}$$

(for a generalization of this map [Huse]). Now we have the following result regarding the points of finite order in the group  $E(K)$ :

- Prop 4:** Let  $E/K$  be an elliptic curve and  $m \geq 1$  an integer relatively prime to  $\text{char}(K)$ .
- (a) The subgroup  $E_1(K)$  has no non-trivial points of order  $m$ .
  - (b) If the reduced curve  $\tilde{E}/K$  is non-singular, then the reduction map

$$E(K)[m] \rightarrow \tilde{E}(k)$$

is injective. (Here  $E(K)[m]$  denotes the set of points of order  $m$  in  $E(K)$ ). where  $E_1 = \{P \in E(K) : \tilde{P} = \tilde{O}\}$ .

#### Good And Bad Reduction:

**Def :** Let  $E/K$  be an elliptic curve, and let  $\tilde{E}$  be the reduced curve for a minimal Weierstrass equation.

- (a)  $E$  has *good(stable) reduction over  $K$*  if  $\tilde{E}$  is nonsingular.
- (b)  $E$  has *multiplicative (or semistable) reduction over  $K$*  if  $\tilde{E}$  has a node [Abh] [Chah].
- (c)  $E$  has *additive (or unstable) reduction over  $K$*  if  $\tilde{E}$  has a cusp [Abh] [Chah] [Men1].

Even if an elliptic curve  $E/K$  has bad reduction, it is often useful to know whether it attains good reduction over some extension of  $K$ . We give this property a name:

**Def :** let  $E/K$  be an elliptic curve.  $E$  has *potential good reduction over  $K$*  if there is a finite extension  $K'/K$  so that  $E$  has good reduction over  $K'$ .

**Example :** If  $K$  is finite extension of  $\mathbb{Q}_p$ , and if  $E/K$  has complex multiplication, then  $E$  has potential good reduction over  $K'$ .

**Prop 5:**(Semi-stable reduction theorem) Let  $E/K$  be an elliptic curve.

- (a) Let  $K'/K$  be an unramified extension. Then the reduction type of  $E$  over  $K$  (i.e good, multiplicative or additive) is the same as the reduction type of  $E$  over  $K'$ .

- (b) Let  $K'/K$  be any finite extension. If  $E$  has either good or multiplicative reduction over  $K$ , then it has the same type of reduction over  $K'$ .
- (c) There exists a finite extension  $K'/K$  so that  $E$  has either good (or split) multiplicative reduction over  $K'$ .

Now we have an important proposition to follow:

**Prop 6:** Let  $E/K$  be an elliptic curve. Then  $E$  has potential good reduction if and only if its  $j$ -invariant is integral (i.e if  $j(E) \in \mathcal{O}_K$ ).

From here on, we will change our perspective and consider the set of elliptic curves as a whole. We will take the collection of all (isomorphism classes of) elliptic curves and make it into an algebraic curve, a so called *modular curve*. Then by studying functions and differential forms on this modular curve, we will be able to make deductions about elliptic curves. Even though this is the way one goes about building the theory of elliptic curves in usual texts [Lang3] [Huse] [Silv1] [Silv2] we will here see only those results which are required to reach or to say understand our final result concerned with the construction of elliptic curves of given group order over a chosen finite field.

Firstly recall that a lattice  $\Lambda \subseteq \mathbb{C}$  defines an elliptic curve  $E/\mathbb{C}$  via the complex analytic map:

$$\begin{aligned} \mathbb{C} &\rightarrow E_{\Lambda}(\mathbb{C}) : y^2 = 4x^3 - g_2x - g_3 \\ z &\rightarrow (\wp(z, \Lambda), \wp'(z, \Lambda)) \end{aligned}$$

Here the Weierstrass  $\wp$ -function relative to the lattice  $\Lambda$ :

$$\wp(z, \Lambda) = z^{-2} + \sum_{\omega \in \Lambda} ((z - \omega)^{-2} + \omega^{-2})$$

Further if  $\Lambda_1$  and  $\Lambda_2$  are two lattices, then we have

$$E_{\Lambda_1} \cong E_{\Lambda_2}$$

( $\mathbb{C}$ -isomorphism) iff  $\Lambda_1$  and  $\Lambda_2$  are homothetic. (Recall that  $\Lambda_1$  and  $\Lambda_2$  are homothetic if there is a number  $c \in \mathbb{C}^*$  such that  $\Lambda_1 = c\Lambda_2$ ). Thus the set of elliptic curves over  $\mathbb{C}$  is intimately related to the set of lattices in  $\mathbb{C}$ , which we denote by  $\mathcal{L}$ :

$$\mathcal{L} = \{\text{lattices in } \mathbb{C}\}$$

We let  $\mathbb{C}^*$  act on  $\mathcal{L}$  by multiplication

$$c\Lambda = \{c\omega : \omega \in \Lambda\}$$

Then the above discussion may be summarized by saying that there is an injection

$$\mathcal{L}/\mathbb{C}^* \rightarrow \frac{\{\text{elliptic curves defined over } \mathbb{C}\}}{\{\mathbb{C} - \text{isomorphism}\}}$$

According to the Uniformization Theorem this map is a bijection. We will need to describe the set  $\mathcal{L}/\mathbb{C}^*$  more precisely. We will put a complex structure on  $\mathcal{L}/\mathbb{C}^*$  and ultimately have that it is isomorphic to  $\mathbb{C}$ . Let  $\Lambda \in \mathbb{C}$ . We can describe  $\Lambda$  by the basis, say  $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ . Switching  $\omega_1$  and  $\omega_2$  if necessary, we always assume that the pair  $(\omega_1, \omega_2)$  gives a positive orientation (that is the angle from  $\omega_1$  to  $\omega_2$  is positive and between 0 and 180. Since we only care about  $\Lambda$  upto homothety, we can normalize our basis by looking instead at [Silv2] [Alf]:

$$1/\omega_2\Lambda = \mathbb{Z}\omega_1/\omega_2 + \mathbb{Z}$$

Our choice of orientation implies that the imaginary part of  $\omega_1/\omega_2$  satisfies  $\text{Im}(\omega_1/\omega_2) > 0$ , which suggests looking at the half plane  $\mathbb{H} = \{\tau \in \mathbb{C} : \text{Im}(\tau) > 0\}$ . We have just seen that the natural map

$$\begin{aligned} \mathbb{H} &\rightarrow \mathcal{L}/\mathbb{C}^* \\ \tau &\rightarrow \Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z} \end{aligned}$$

is surjective. It is not, however injective. When do two  $\tau$ 's give the same lattice?:

**Prop 7:**(a) Let  $\Lambda \subset \mathbb{C}$  be a lattice, and let  $\omega_1, \omega_2$  and  $\omega'_1, \omega'_2$  be two oriented basis for  $\Lambda$ . Then

$$\begin{aligned} \omega'_1 &= a\omega_1 + b\omega_2 \\ \omega'_2 &= c\omega_1 + d\omega_2 \end{aligned}$$

for some  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ .

(b) Let  $\tau_1, \tau_2 \in \mathbb{H}$ . Then  $\Lambda_{\tau_1}$  is homothetic to  $\Lambda_{\tau_2}$  iff there is a  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$  such that

$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}$$

(c) Let  $\Lambda \subset \mathbb{C}$  be a lattice. Then there is a  $\tau \in \mathbb{H}$  such that  $\Lambda$  is homothetic to  $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$

And hence, we have that to each  $\tau \in \mathbb{H}$  we have associated a lattice  $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$  and an elliptic curve  $\mathbb{C}/\Lambda_\tau$ .

The (modular) discriminant is the function

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$$

The modular  $j$ -invariant  $j(\tau)$  is the function

$$j(\tau) = \frac{1728g_2(\tau)^3}{\Delta(\tau)}$$

Thus  $j(z)$  is the  $j$ -invariant of the elliptic curve

$$E_{\Lambda_\tau} : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

and  $E_{\Lambda_\tau}(\mathbb{C})$  has a parametrization using the Weierstrass  $\wp$ -function:

$$\begin{aligned} \mathbb{C}/\Lambda_\tau &\rightarrow E_{\Lambda_\tau}(\mathbb{C}) \\ z &\rightarrow (\wp(z, \Lambda_\tau), \wp'(z, \Lambda_\tau)) \end{aligned}$$

Now let us finally look into the Uniformization Theorem for elliptic curves over  $\mathbb{C}$  again. Let  $A, B \in \mathbb{C}$  satisfy  $4A^3 + 27B^2 \neq 0$ . Then there is a unique lattice  $\Lambda \subset \mathbb{C}$  such that

$$g_2(\Lambda) = 60G_4(\Lambda) = -4A$$

$$g_3(\Lambda) = 140G_6(\Lambda) = -4B$$

The map

$$\begin{aligned} \mathbb{C}/\Lambda &\rightarrow : y^2 = x^3 + Ax + B \\ z &\rightarrow (\wp(z, \Lambda), \wp'(z, \Lambda)) \end{aligned}$$

We are now ready to relate the function  $j(\tau)$ , defined as a meromorphic function on the Riemann Surface (the modular curve) to the  $j$ -invariant defined w.r.t the Weierstrass equation as  $c_4^2/\Delta$  which classifies isomorphism classes of elliptic curves. We let

$$\mathcal{ELL}_{\mathbb{C}} = \frac{\{\text{elliptic curves defined over } \mathbb{C}\}}{\{\mathbb{C}\text{-isomorphism}\}}$$

Thus the element of  $\mathcal{ELL}_{\mathbb{C}}$  is a  $\mathbb{C}$ -isomorphism class of elliptic curves. We also recall the notation

$$\mathcal{L} = \{\text{lattices in } \mathbb{C}\}$$

Much of our preceding discussion is summarized in the following proposition: There is a one-to-one correspondence between the following four sets, given by the indicated maps: Here  $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ ,  $\{E_\Lambda\}$  denotes the isomorphism class of the elliptic curves  $E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$  and  $\{\Lambda\}$  is the homothety class of the lattice  $\Lambda$ .

Let us describe in a bit more detail the bijective map

$$\mathcal{ELL} \rightarrow \mathbb{C}$$

given in the above proposition. Let  $\{E\} \in \mathcal{ELL}_{\mathbb{C}}$  be an isomorphism class of elliptic curves, and choose a Weierstrass equation

$$E : y^2 = x^3 + Ax + B$$

for some curve  $E$  in this class. Now take a basis  $\gamma_1, \gamma_2$  for the homology group  $\mathcal{H}_1(E(\mathbb{C}), \mathbb{Z})$  and compute the periods [Silv2]

$$\omega_1 = \int_{\gamma_1} \frac{dx}{y} \text{ and } \omega_2 = \int_{\gamma_2} \frac{dx}{y}$$

switching  $\omega_1$  and  $\omega_2$  if necessary, we may assume that

$$\tau_E = \frac{\omega_1}{\omega_2} \in \mathbb{H}$$

Then evaluate the holomorphic function  $j(\tau)$  at  $\tau = \tau_E$ . Thus the map

$$j : \mathcal{ELL}_{\mathbb{C}} \rightarrow \mathbb{C}, \{E\} \rightarrow j(\tau_E)$$

involves two transcendental (i.e non-algebraic) operations, namely the computation of the periods  $\omega_1, \omega_2$  and the evaluation of the function  $j(\tau)$ . From this perspective, it seems unlikely that the rationality properties of  $j(\tau_E)$  should have anything to do with rationality properties of  $E$ . To describe the relationship that does exist, we make the following definitions.

**Def :** Let  $\{E\} \in \mathcal{ELL}_{\mathbb{C}}$ , and let  $K \subseteq \mathbb{C}$ . We say that  $K$  is a field of definition for  $\{E\}$  if there is an elliptic curve  $E_0$  in the isomorphism class  $\{E\}$  such that  $E_0$  is defined over  $K$ . We say that  $K$  is a *field of moduli* for  $\{E\}$  if for all automorphisms  $\sigma \in \text{Aut}(\mathbb{C}/\mathbb{Q})$ ,

$$E^\sigma \in \{E\}$$

iff  $\sigma$  acts trivially on  $K$ . Note that the field of moduli exists and is unique. Since by Galois Theory, an equivalent definition is that the field of moduli is the fixed field of the group [Silv2] [Lang1]:

$$\{\sigma \in \text{Aut}(\mathbb{C}/\mathbb{Q}) : E^\sigma \in \{E\}\}$$

From the complex analytic viewpoint described above, it is not clear that the number  $j(\{E\})$  should have any relationship to fields of definition and moduli for  $\{E\}$ . Note that there are lots of bijections  $\mathcal{ELL} \rightarrow \mathbb{C}$ . We have the following proposition about the field of moduli for  $\{E\}$ .

**Prop 8:** Let  $\{E\} \in \mathcal{ELL}_{\mathbb{C}}$ .

(a)  $\mathbb{Q}(j(\{E\}))$  is the field of moduli for  $\{E\}$ .

(b)  $\mathbb{Q}(j(\{E\}))$  is the minimal field of definitions for  $\{E\}$ .

Now, in the next section, let us introduce ourselves with one the most important and beautiful topics in not only mathematics but of entire science as a whole [BCIS] [Silv2] [Shaf2], which leads to our problem of construction of curves.

## 2.3 Complex Multiplication

Most elliptic curves over  $\mathbb{C}$  have only the *multiplication by  $m$*  endomorphisms. An elliptic curve that possesses extra endomorphisms is said to have *Complex Multiplication* or *CM* for short. Such curves have many properties. For example, the endomorphism ring of a *CM* curve  $E$  is an *order* in a imaginary quadratic field  $K$ , and the  $j$ -invariant and torsion points of  $E$  generate abelian extensions of  $K$ . (This analogous to the way in which the torsion points of  $\mathcal{G}_m(\mathbb{C}) = \mathbb{C}^*$  generate abelian extensions of  $\mathbb{Q}$ ). An important result in the cyclotomic theory [Shaf2] [Chah] [Lang2] is the *Kronecker-Weber* theorem, which says that every abelian extension of  $\mathbb{Q}$  is contained in a cyclotomic extension. We will see the corresponding results for a imaginary quadratic field  $K$ . The most important of which, we will see is how to construct an elliptic curve such that  $K(j(E))$  is the *Hilbert Class Field* of  $K$ , and we will see how to use the torsion points of  $E$  to generate the maximal extension of  $K$ . (the main prerequisite to this section is some familiarity with basic theorems of Class Field Theory. (For those without such an exposure, assuming the end results would suffice)

### Complex Multiplication of curves over $\mathbb{C}$ :

Let  $E/\mathbb{C}$  be an elliptic curve with complex multiplication. We know from [BCIS] [Silv1] that  $\text{End}(E) \otimes \mathbb{Q}$  is isomorphic to a quadratic imaginary field and that  $\text{End}(E) \cong \mathcal{O} \subset \mathbb{C}$  and  $K = \mathcal{O} \otimes \mathbb{Q}$ , then we will say that  $E$  has *complex multiplication by  $\mathcal{O}$*  or that  $E$  has *CM by  $K$* . We also let

$$\mathcal{O}_K = \text{ring of integers(maximal order) of } K$$

Much of the theory becomes easier if one restricts attention to elliptic curves with *CM* by  $\mathcal{O}_K$ , so we will usually take this course.

We have seen in the previous sections that in order to understand particular elliptic curves, it is often useful to study the set of all elliptic curves with *CM*. Similarly, in order to study a particular elliptic curve with *CM*, it turns out that one should look at the set of all elliptic curves with the same endomorphism ring. Of course, by *elliptic curves* we really mean isomorphism classes of elliptic curves, which lead us to define:

$$\mathcal{ELL}(\mathcal{O}) = \frac{\{\text{elliptic curves with } \text{End}(E) \cong \mathcal{O}\}}{\text{isomorphism over } \mathbb{C}}$$



$$= \frac{\{\text{lattices } \Lambda \text{ in } \mathbb{C}\}}{\text{homothety}}$$

If we start with a imaginary quadratic field  $K$ , how might we construct an elliptic curve with  $CM$  by  $\mathcal{O}_K$ ?. If  $\mathcal{A}$  is a non zero ideal of  $\mathcal{O}_K$  or more generally if it is a fractional ideal of  $K$ , then using the embedding  $\mathcal{A} \subset K \subset \mathbb{C}$  we see that  $\mathcal{A}$  is a lattice in  $\mathbb{C}$ . (This is clear from the definition of fractional ideals[Heck][Cohn1][Shaf2][Lang2][PoZe], which for quadratic imaginary fields implies that  $\mathcal{A}$  is a  $\mathbb{Z}$ -module of rank 2 which is not contained in  $\mathbb{R}$ . Hence we form an elliptic curve  $E_{\mathcal{A}}$  whose endomorphism ring is

$$\begin{aligned} \text{End}(E_{\mathcal{A}}) &\cong \{\alpha \in \mathbb{C} : \alpha\mathcal{A} \subset \mathcal{A}\} \\ &= \{\alpha \in K : \alpha\mathcal{A} \subset \mathcal{A} \text{ since } \mathcal{A} \subset K\} \\ &= \mathcal{O}_K \text{ since } \mathcal{A} \text{ is a fractional ideal.} \end{aligned}$$

Thus each nonzero fractional ideal  $\mathcal{A}$  of  $K$  will give an elliptic curve with  $CM$  by  $\mathcal{O}_K$ . On the other hand, since homothetic lattices give isomorphic elliptic curves, we see that  $\mathcal{A}$  and  $c\mathcal{A}$  give the same curve in  $\mathcal{ELL}(\mathcal{O}_K)$ . This suggests that we look at the group of fractional ideals modulo principal ideals which, the reader may recognize as one of the fundamental objects of study in *algebraic number theory*:

$$\begin{aligned} \mathcal{CL}(\mathcal{O}_K) &= \text{ideal class group of } \mathcal{O}_K. \\ &= \frac{\{\text{nonzero fractional ideals of } K\}}{\{\text{nonzero principal ideals of } K\}} \end{aligned}$$

If  $\mathcal{A}$  is a fractional ideal of  $K$ , we denote  $\mathcal{A}'$  its ideal class in  $\mathcal{CL}(\mathcal{O}_K)$ . We have seen that there is a map

$$\begin{aligned} \mathcal{CL}(\mathcal{O}_K) &\rightarrow \mathcal{ELL}(\mathcal{O}_K) \\ \mathcal{A}' &\rightarrow E_{\mathcal{A}} \end{aligned}$$

More generally, if  $\Lambda$  is any lattice with  $E_{\Lambda} \in \mathcal{ELL}(\mathcal{O}_K)$  and  $\mathcal{A}$  is any nonzero fractional ideal of  $K$ , we can form the product:

$$\mathcal{A}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r : \alpha_i \in \mathcal{A}, \lambda_i \in \Lambda\}$$

Now, we have an elementary but crucial fact that this induces a simply transitive action of the ideal class group  $\mathcal{CL}(\mathcal{O}_K)$  on the set of elliptic curves  $\mathcal{ELL}(\mathcal{O}_K)$ . This proposition forms the basis for all of our subsequent results on  $CM$ :

**Prop 9:**(a) Let  $\Lambda$  be a lattice with  $E_{\Lambda} \in \mathcal{ELL}(\mathcal{O}_K)$ , and  $\mathcal{A}$  and  $\mathcal{B}$  be nonzero fractional ideals of  $K$ .

(i)  $\mathcal{A}\Lambda$  is a lattice in  $\mathbb{C}$ .

(ii) The elliptic curve  $E_{\mathcal{A}\Lambda}$  satisfies  $\text{End}(E_{\mathcal{A}\Lambda}) \cong \mathcal{O}_K$

(iii)  $E_{\mathcal{A}\Lambda} \cong E_{\mathcal{B}\Lambda}$  iff  $\mathcal{A}' = \mathcal{B}'$  in  $\mathcal{CL}(\mathcal{O}_K)$ .

Hence there is a well defined action of  $\mathcal{CL}(\mathcal{O}_K)$  on  $\mathcal{ELL}(\mathcal{O}_K)$  determined by

$$\mathcal{A} * E_{\Lambda} = E_{\mathcal{A}^{-1}\Lambda}$$

(b) The action of  $\mathcal{CL}(\mathcal{O}_K)$  on  $\mathcal{ELL}(\mathcal{O}_K)$  described in (a) is simply transitive. In particular,

$$\#\mathcal{CL}(\mathcal{O}_K) = \#\mathcal{ELL}(\mathcal{O}_K)$$

Now, let us look into a proposition which says that every elliptic curve with  $CM$  is defined over an algebraic extension of  $\mathbb{Q}$ .

**Prop 10:**(a) Let  $E/\mathbb{C}$  be an elliptic curve, and let  $\sigma : \mathbb{C} \rightarrow \mathbb{C}$  be any field automorphism of  $\mathbb{C}$ . Then

$$\text{End}(E^{\sigma}) \cong \text{End}(E)$$

(b) Let  $E/\mathbb{C}$  be an e. c with  $CM$  by the ring of integers  $\mathcal{O}_K$  of a imaginary quadratic field  $K$ . Then  $j(E) \in \mathbb{Q}'$ . (Later we will see that  $j(E)$  is an algebraic integer i. e  $\in \mathbb{Z}'$ .)

(c)

$$\mathcal{ELL} \cong \frac{\{\text{elliptic curves } E/\mathbb{Q}' \text{ with } \text{End}(E) \cong \mathcal{O}_K\}}{\text{isomorphism over } \mathbb{Q}'}$$

Since till now we looked into the results in the theory of  $CM$ , which provide the crucial link between  $\mathcal{ELL}(\mathcal{O})$  and lattices in  $\mathbb{C}$ , we now take recourse to Class Field Theory, which provides us with the actual explicit link. Here again, we will be concerned about the end results and not the intricacies involved in Class Field Theory. (That is we will just see only what Class Field Theory says about our problem) But the reader is strongly advised to look into [Cohn1] [BCIS] for all the basic material.

## 2.4 Class Field Theory : A Brief Review

Class Field Theory describes the abelian extensions of a number field  $K$  in terms of the arithmetic of  $K$ . The theory of  $CM$  provides an analytic realization of class field theory for imaginary quadratic fields, much as cyclotomic theory gives a realization of class field theory for  $\mathbb{Q}$  (*Kronecker-Weber* theorem). We will here look into the classical version using ideals and ideal class groups. We will restrict our attention to totally imaginary quadratic fields, that is, fields with no real embeddings, since that is the only case we will use in the sequel.

Let  $K$  be a totally imaginary quadratic number field and let  $L$  be a finite abelian extension of  $K$ , that is  $L/K$  is Galois with abelian Galois group. As usual, we write  $\mathcal{O}_K$  and

$\mathcal{O}_L$  for the rings of integers (maximal orders) of  $K$  and  $L$  respectively. Let  $\mathcal{P}$  be a prime of  $K$  which does not ramify in  $L$ , and let  $\mathcal{B}$  be a prime of  $L$  lying over  $\mathcal{P}$  [PoZe] [Lang2] [Heck] [Shaf2] Thus the picture is

$$\begin{aligned} L &\rightarrow K \text{ (finite abelian extension)} \\ \mathcal{P} &\rightarrow \mathcal{B} \text{ (unramified prime)} \\ \mathcal{O}_K/\mathcal{P} &\rightarrow \mathcal{O}_L/\mathcal{B} \text{ (extension of finite fields)} \end{aligned}$$

By restriction, we get a homomorphism from the decomposition group of  $\mathcal{B}$  to the Galois group of the residue fields:

$$\{\sigma \in \text{Gal}(L/K) : \mathcal{B}^\sigma = \mathcal{B}\} \rightarrow (\text{Galois group of } \mathcal{O}_L/\mathcal{B} \text{ over } \mathcal{O}_K/\mathcal{P})$$

The right hand Galois group is cyclic, generated by the *Frobenious Endomorphism*:

$$x \rightarrow x^{\text{N}_{\mathbb{Q}^P}^K}$$

Further, since  $\mathcal{P}$  is unramified, there is a unique element  $\sigma_{\mathcal{P}} \in \text{Gal}(L/K)$  which maps to *Frobenious Endomorphism*. The notation reflects the fact that  $\sigma_{\mathcal{P}}$  is determined by the prime ideal  $\mathcal{P}$  in  $K$ . For a general Galois extension  $L/K$ ,  $\mathcal{P}$  will only determine the conjugacy class of  $\sigma_{\mathcal{P}}$ , and making a new choice for  $\mathcal{B}$  will change  $\sigma_{\mathcal{P}}$  by conjugation. But in our situation  $\sigma_{\mathcal{P}}$  will not change, since we have assumed that  $L/K$  is abelian. Thus  $\sigma_{\mathcal{P}} \in \text{Gal}(L/K)$  is uniquely determined by the condition

$$\sigma_{\mathcal{P}}(x) \equiv x^{\text{N}_{\mathbb{Q}^P}^K} \pmod{\mathcal{B}} \forall x \in L$$

After the following theorem, we reach the most important theorem needed by us to develop a procedure to design an elliptic curve of given group order over large finite fields.

**Theorem** : Let  $K/\mathbb{Q}$  be an imaginary quadratic field with ring of integers  $\mathcal{O}_K$ , and let  $E/\mathbb{C}$  be an elliptic curve with  $\text{End}(E) \cong \mathcal{O}_K$ . Then  $K(j(E))$  is the *Hilbert Class Field*  $\mathcal{H}$  of  $K$ . (For the definition of Hilbert Class Field, please see [BCIS] [Cohn1] [Shaf1] [Shaf2] [Heck]).

**Remark** : Note that it is easy to have a curve whose endomorphism ring is  $\mathcal{O}_K$ . For example, we could take  $E$  to be the curve corresponding to the lattice  $\mathcal{O}_K$ . Then

$$j(E) = j(\mathcal{O}_K) = 1728 \frac{g_2(\mathcal{O}_K)^3}{g_2(\mathcal{O}_K)^3 - 27g_3(\mathcal{O}_K)^2}$$

is given in terms of series  $g_2(\mathcal{O}_K)$  and  $g_3(\mathcal{O}_K)$  involving the elements of  $\mathcal{O}_K$ . Alternatively, if we write  $\mathcal{O}_K = \mathbb{Z}\tau + \mathbb{Z}$ , then

$$j(E) = j(\mathcal{O}_K) = e^{-2\pi i \tau} + \sum_{n=0}^{\text{infinty}} c(n) e^{2\pi i n \tau}$$

where the  $c(n) \in \mathbb{Z}$  are the coefficients in the  $q$ -series expansion of  $j$ [Silv2] [AtMo]. So the above theorem says that the Hilbert Class Field of a quadratic imaginary field  $K$  is generated by the value of a certain holomorphic function  $j(\tau)$  evaluated at a generator for the ring of integers of  $K$ .

We now have the final result , which says much more than the mere statement of the above theorem:

**Theorem** :let  $E$  be an elliptic curve representing an isomorphism class in  $\mathcal{ELC}(\mathcal{O}_K)$ .

(a)  $K(j(E))$  is the Hilbert Class Field  $\mathcal{H}$  of  $K$ .

(b)  $[\mathbb{Q}(j(E)):\mathbb{Q}]=[K(j(E)) : K]=h_K$ . where  $h_K = \#\mathcal{CL}(\mathcal{O}_K) = \#Gal(\mathcal{H}/K)$  is the class number of  $K$ .

(c) Let  $E_1, \dots, E_h$  be a complete set of represents for  $\mathcal{ELC}(\mathcal{O}_K)$ . Then  $j(E_1), \dots, j(E_h)$  is a complete set of  $Gal(K'/K)$  conjugates for  $j(E)$ .

(d) For every prime ideal  $\mathcal{P}$  of  $K$ ,

$$j(E)^{\sigma_{\mathcal{P}}} = j(\mathcal{P}' * E)$$

More generally, for every nonzero fractional ideal  $\mathcal{A}$  of  $K$ ,

$$j(E)^{(\mathcal{A}, \mathcal{H}/K)} = j(\mathcal{A}' * E)$$

Finally, we have:

**Theorem** :  $j(E)$  is an algebraic number. i.  $e \in \bar{\mathbb{Z}}$ .

The reader is referred to [Cohn1] [BCIS] [Shaf2] [Shaf1] for the material concerned with Class Fields and Ring Class Fields.

## 2.5 Class Invariants

Before looking into what class invariants are, let us look into the notion of complex multiplication once again briefly.

The notion of complex multiplication: Let  $E$  be an elliptic curve. As a complex Lie group, it is the quotient of the complex plane  $\mathbb{C}$  by a lattice  $\Lambda$ , spanned by two periods  $\omega_1, \omega_2$  and since  $E$  is isomorphic to the curve defined by the periods  $z\omega_1, z\omega_2$  for any nonzero  $z \in \mathbb{C}$  we may assume  $\Lambda$  to be spanned by 1 and  $\tau$ , where  $\tau$  has a positive imaginary part.

An endomorphism of  $E$  may be identified with an endomorphism of its universal covering  $\mathbb{C}$  mapping  $\Lambda$  into itself; it is therefore the multiplication by a complex number  $z$  such

that  $z, z\tau \in \Lambda$ . The endomorphisms of  $E$  form a ring  $\text{End}(E)$ , which always contains the integers  $\mathbb{Z}$ , (the *trivial endomorphisms*). The other ones (if any) are given by complex numbers and are called *Complex Multiplications*. If  $\text{End}(E) \neq \mathbb{Z}$ , the curve is said to admit complex multiplications.

In general,  $E$  has no CM. In fact, assume that  $z$  defines a non trivial endomorphism of  $E$ . Then

$$z = a + b\tau, \quad z\tau = c + d\tau, \quad (a, b, c, d \text{ integers}, b \neq 0),$$

whence

$$a\tau + b\tau^2 = c + d\tau$$

and  $\tau$  must belong to an imaginary quadratic field, say  $K$ ; moreover  $z$  belongs to the ring of integers  $\mathcal{O}_K$  of  $K$  since it is in  $K$  and defines an endomorphism of a  $\mathbb{Z}$ -module of finite rank, namely  $\Lambda$ . Therefore,  $\text{End}(E)$  is an order of  $K$ , (subring of  $\mathcal{O}_K$  containing  $z$  and which has rank 2 as a  $\mathbb{Z}$ -module); one gets in this way all orders of all quadratic imaginary fields (if  $\mathcal{O}$  is such an order, take for a curve  $E$  with lattice of periods  $\mathcal{O}$ ; since  $1 \in \text{cal } \mathcal{O}$ ,  $z\mathcal{O} \subset \mathcal{O}$  iff  $z \in \mathcal{O}$ , whence  $\text{End}(E) = \mathcal{O}$ ).

Assume that  $\text{End}(E) = \mathcal{O}_K$ , and that  $\Lambda \subset K$ . Then  $\Lambda$  is an ideal of  $K$ , and conversely any ideal of  $K$  gives rise to a curve  $E$  such that  $\text{End}(E) = \mathcal{O}_K$ . Two such curves are homothetic, i.e. belong to the same *ideal class*.

Let  $j$  be the modular function. For the curve with normal equation:

$$y^2 = 4x^3 - g_2x - g_3$$

its value is

$$j = 1728g_2^3/\Delta, \quad (\Delta = g_2^3 - 27g_3^2)$$

Two elliptic curves are isomorphic over an algebraically closed field iff their modular invariants are equal. By the above,  $j$  defines a function on the *ideal classes*  $\mathcal{A}_1, \dots, \mathcal{A}_h$  of  $K$ ; the numbers  $j(\mathcal{A}_i)$  are *singular values* of  $j$ , and are called the *Class Invariants* of  $K$ ; they are pairwise different, and have proved to be of fundamental importance in the study of abelian extensions of  $K$ . Now let us see some important theorems (we have already seen them but here we are restating them in terms of the Class Invariants just defined):

**Theorem 1:** *The class invariants  $j(\mathcal{A}_i)$  are algebraic numbers i.e. they belong to  $\mathcal{O}_K$ .*

**Theorem 2:**  *$K(j(\mathcal{A}_i))$  is independent of  $i$ , ( $1 \leq i \leq h$ ), and is the maximal unramified abelian extension of  $K$ .*

(Unramified means that every prime ideal of  $K$  decomposes in a product of distinct prime ideals with exponent 1. )

By Class Field Theory, it is known that the maximal unramified abelian extension of  $K$  (Hilbert's *absolute class field*) exists and that its Galois group  $G_K$  is canonically isomorphic to the group  $C_K$  of ideal classes; the next theorem describes how it operates on the  $j(\mathcal{A}_K)$ .

**Theorem 3:** *Let  $\mathcal{A} \in \mathcal{CL}(\mathcal{O}_K)$  and let  $\sigma_{\mathcal{A}} \in G_K$  be its image by the isomorphism of Class Field Theory. Then*

$$\sigma_{\mathcal{A}}(j(\mathcal{A}_i)) = j(\mathcal{A}^{-1} \cdot \mathcal{A}_i) .$$

## 2.6 Weber's Class Invariants:

Till now i.e. in all our of previous discussions, we saw results concerned with elliptic curves which admit  $CM$  and whose endomorphism ring  $End(E)$  is the whole of the ring of integers  $\mathcal{O}_K$  of  $K$  (i.e the maximal order of  $K$ ). But as we will see, for our problem of construction of elliptic curves it is the ring class field  $H_{\mathcal{O}}$  associated to an order  $\mathcal{O} \subset \mathcal{O}_K$  of  $K$  and not allways the class field associated to the maximal order  $\mathcal{O}_K$  that is actually needed. For which, we will look into the way Weber has extended the concept (rather generalized) the concept of what Class Invariants are. Before that let us recall again, some basic definitions:

The *modular group* and *modular invariant*  $j$ :

The *modular group* is defined to be  $\Gamma = SL_2(\mathbb{Z})/\{\pm 1\}$ . An element  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  of  $\Gamma$  acts on  $\mathbb{H} = \{z \in \mathbb{C}, Im(z) > 0\}$  by

$$gz = \frac{az + b}{cz + d}$$

It is known that  $\Gamma$  is generated by  $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and  $T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .

A *modular form* of weight  $2k$  ( $k$  any integer) is a function meromorphic everywhere on  $\mathbb{H}$  and at infinity, satisfying:

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \forall z \in \mathbb{H},$$

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right)$$

If the form is holomorphic everywhere (which implies  $k > 0$  for nonconstant forms), we say that the form is *regular*. A form of weight 0 is called a *modular function*.

Let  $\Lambda(1, \omega) = \mathbb{Z} + \omega\mathbb{Z}$  be a lattice in  $\mathbb{C}$  ( $\omega \in \mathbb{H}$ ). Put

$$G_{2k}(\Lambda) = \sum_{(m,n) \neq (0,0)} \frac{1}{(m\omega + n)^{2k}},$$

for  $k > 1$ , then  $G_{2k}(\Lambda)$  is a *regular* modular form of weight  $2k$ . We put  $g_2(\Lambda) = 60G_4$ ,  $g_3(\Lambda) = 140G_6$  and  $\Delta = g_2^3 - 27g_3^2$  : these are regular modular forms of weight 4, 6 and 12, respectively. The *modular invariant*  $j$  is then  $j = 1728g_2^3/\Delta$ . We have the proposition:

**Prop :** The function  $j$  is a modular function (i.e. a modular form of weight 0), is holomorphic in  $\mathbb{H}$ , and has a simple pole at infinity. The function  $j$  is a complex analytic isomorphism from  $\mathbb{H}/\Gamma$  to  $\mathbb{C}$ .

Let  $K$  be an imaginary quadratic field,  $\mathcal{O}_K$  its ring of integers(maximal order) of  $K$ . The discriminant of  $K$  is the discriminant of  $\mathcal{O}_K$  and the discriminant of any order  $\mathcal{O} \subset \mathcal{O}_K$  in  $K$  is given by

$$D[\mathcal{O}] = D[\mathcal{O}_K] \cdot f^2(\mathcal{O})$$

if  $1, \omega$  ( $\omega \in \mathcal{O}_K$ ) is a integral basis for  $\mathcal{O}$  i.e.  $\mathcal{O} = [1, \omega] = \mathbb{Z} + \omega\mathbb{Z}$  and  $\mathcal{O}_K = [1, \omega_K] = \mathbb{Z} + \omega_K\mathbb{Z}$ , then

$$D[\mathcal{O}] = D[\mathcal{O}_K] \cdot f^2(\omega)$$

where the positive quantity  $f(\omega)$  is defined as the *ring-index* of  $\omega$  because.  $f(\omega) = f(\mathcal{O}) = [\mathcal{O}_K : \mathcal{O}]$ . That is,  $\mathcal{O}_K$  can be viewed as a Dedekind extension of  $\mathcal{O}$  of index of extension  $[\mathcal{O}_K : \mathcal{O}] = f(\mathcal{O}) = f(\omega)$ . It can be shown that if  $\mathcal{O}_K = [1, \omega_K]$ , then any order  $\mathcal{O} \subset \mathcal{O}_K$  in  $K$  is given by  $\mathcal{O} = [1, \omega] = [1, f(\omega) \cdot \omega_K]$ . That is,  $\mathcal{O} = \mathbb{Z} + [\mathcal{O}_K : \mathcal{O}]\omega_K\mathbb{Z}$ .

Now, let  $u(z)$  denote a modular function(i.e a modular form of weight 0) and  $\omega = \omega(\mathcal{O})$  be the generator of  $\mathcal{O}$  such that  $\mathcal{O} = \mathbb{Z} + \omega\mathbb{Z} = \mathbb{Z} + [\mathcal{O}_K : \mathcal{O}]\omega_K\mathbb{Z}$ , where  $\omega_K = \omega(\mathcal{O}_K)$ . *Weber calls  $u(\omega)$  a Class Invariant* if  $u(\omega) \in H_{\mathcal{O}} = K(j(\omega))$  the ring class field associated to the order  $\mathcal{O} = [1, \omega]$ .

Since, we can construct Class Invariants which belong to the ring class field  $H_{\mathcal{O}}$ , associated to an order  $\mathcal{O}$  in  $K$ , our strategy to find the  $j$ -invariant  $j(\omega)$  and hence an elliptic curve having a given group order over a large finite field (since the  $j$ -invariant determines a curve uniquely upto isomorphism) would be to construct suitable Class Invariants  $u(\omega)$  which are functions of  $j(\omega)$  and whose minimal polynomials can be found indirectly (i.e. can be computed easily) solve the minimal polynomial and to get  $u = u(\omega)$  and use the relation between  $u(\omega)$  and  $j(\omega)$  to get  $j(\omega)$ . We will see the details of this in the next chapter, in the design section. For examples of Weber Class Invariants, the reader is referred to [AtMo].

## Chapter 3

# Optimal Normal Basis

We know that by representing the elements of  $\text{GF}(2^n)$  ( $\text{GF}(p^n)$  in general) in terms of a normal basis, the arithmetic operations in that field can be simplified (that is, made almost free) because, we can re-interpret them in terms of shifts (which amounts to squaring in  $\text{GF}(2^n)$ ) and additions (mod 2 or mod  $p$ ) of the coordinate vectors of the elements (w.r.t the chosen basis) [Men2] [LidN]. Now let us see if the arithmetic operation of multiplication w.r.t a normal basis representation can be simplified or optimised in the sense of further reducing the computation, that is to say, let us see whether some kind of optimality is feasible or not (defined w.r.t some criterion) because of the nature of the particular normal basis chosen [MOVW]. (for a given field, many exist).

### 3.1 Optimality Criterion

Let  $\{\beta^{2^0}, \beta^{2^1}, \dots, \beta^{2^{n-1}}\}$  be a normal basis(NB) of  $\text{GF}(2^n)$  and elements  $A, B, C$  of  $\text{GF}(2^n)$  in terms of NB be given as :

$$A = \sum_{i=1}^{n-1} a_i \beta^{2^i}, B = \sum_{i=1}^{n-1} b_i \beta^{2^i}$$

$$C = \sum_{i=1}^{n-1} c_i \beta^{2^i} = A \cdot B$$

$$C = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_i b_j \beta^{2^i} \beta^{2^j}$$

Let the cross product terms:

$$\beta^{2^i} \beta^{2^j} = \sum_{k=1}^{n-1} \lambda_{i,j}^{(k)} \beta^{2^k} \quad \lambda_{i,j}^{(k)} \in \mathbb{F}_2$$



substitution yields the following bilinear form for  $c_k$ :

$$c_k = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \lambda_{i,j}^{(k)} a_i b_j$$

$$c_k = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \lambda_{i,j}^{(0)} a_{i+k} b_{j+k}$$

where the subscripts of  $a$  and  $b$  are taken mod  $n$ . [MOVW] Thus we have

$$c_0 = \bar{A} \Lambda \bar{B}^T; \quad \Lambda = (\lambda_{i,j}^{(0)})$$

$$\bar{A} = (a_0, a_1, \dots, a_{n-1})$$

$$\bar{B} = (b_0, b_1, \dots, b_{n-1})$$

$$\bar{C} = (c_0, c_1, \dots, c_{n-1})$$

where  $\bar{B}^T$  is the transpose of  $\bar{B}$ . The remaining coefficients of  $C$  can be found using the same matrix, but with  $\bar{A}$  and  $\bar{B}$  cyclically shifted.

In terms of hardware implementation of the arithmetic operation of multiplication the circuit to compute  $c_0$  also computes  $c_k$  if the registers holding  $\bar{A}$  and  $\bar{B}$  are cyclically shifted  $k$  positions to the left.

Clearly it is useful to define the quantity :

$$C_N = | \{ (i, j) : \lambda_{i,j} \neq 0; 0 \leq i, j \leq n-1 \} |$$

(where  $| S |$  represents the cardinality of the set  $S$ ) which will be referred to as the *Complexity of multiplication w.r.t the normal basis*:

$$NB = \{\beta^{2^0}, \beta^{2^1}, \dots, \beta^{2^{n-1}}\}$$

We have the following bounds for the quantity  $C_N$  :

$$2n - 1 \leq C_N \leq n^2$$

In the design of an IC to implement the multiplication, each nonzero element of  $\Lambda$  corresponds to a cell connection and it is important to find bases of low complexity. (This is the criterion which we were referring to) Bases that achieve the minimum possible complexity for any given value of  $n$  are referred to as *minimal normal bases*. If the minimum complexity is, in fact the theoretical minimum of  $2n - 1$ , then, the minimal NB is called an *Optimal Normal Basis* (uniqueness of which can be easily shown [MOVW]).

## 3.2 Construction of Optimal Normal Bases

There are two types of optimal normal bases (ONBs) depending upon the way they are constructed. They are *Type I* and *Type II* optimal normal bases. It can be shown that these are the only types of ONBs. That is, all ONBs can be constructed by either Type I or Type II (for recent generalizations see [Men2]). Now, let us see what Type I and Type II constructions are [Men2]:

**Type I:** Suppose  $n + 1$  is a prime and  $q$  is primitive in  $\mathbb{Z}_{n+1}^*$ , where  $q$  is a prime or prime power. Then any primitive  $n + 1$ 'st root of unity generates an optimal normal basis (ONB)  $\Rightarrow$  it is an optimal normal basis generator (ONBG).

**Type II:** let  $2n + 1$  be a prime and assume that  $\mathbb{Z}_{2n+1}^*$  is generated by 2 and -1. Then  $\alpha = \gamma + \gamma_{-1}$  generates an optimal normal basis for  $\text{GF}(2^n)$  over  $\text{GF}(2)$ , where  $\gamma$  is a primitive  $(2n + 1)$ st root of unity.

For cryptographic purposes, it is important to have either a primitive element or an element of high multiplicative order in  $\text{GF}(2^n)$ . Since Type II ONBGs have invariably large orders in the range of interest (mostly primitive), if they exist in  $\text{GF}(2^n)$ , we will mostly be interested in the *explicit* construction of Type II only. So let us look into the way we can construct explicitly Type II ONBGs.

## 3.3 Explicit construction of Type II ONBGs

Here by explicit construction, we mean expressing the ONBG in terms of the polynomial basis (standard or power basis) with which the field elements of  $\text{GF}(2^n)$  are expressed. (Here we mean a  $\text{GF}(2^n)$  in which we know that an ONBG exists) That is to say, we want to express the ONBG in terms of the polynomial basis generated by the root of the irreducible polynomial used to construct the field  $\text{GF}(2^n)$ . For which clearly we need the minimal polynomial of the Type II ONBG.

Assuming that  $\beta$  is the Type II ONBG for the field  $\text{GF}(2^n)$  (that is the field in which its existence has been verified by the above stated criteria for the construction of Type II ONBGs) it is easy to derive that the minimal polynomial of  $\beta \rightarrow m_\beta(x)$  is specified in terms of the recursion [Men2]:

$$\begin{aligned} \text{Let } f_0(x) &= 1; \quad f_1(x) = x + 1 \\ f_t(x) &= x f_{t-1}(x) + f_{t-2}(x) \quad t \geq 2 \end{aligned}$$

be the sequence of polynomials  $f_i(x)$   $i = 1, 2, \dots$  over  $\text{GF}(2)$ . Then if  $n$  is such that we have an ONBG guaranteed, then  $f_n(x)$  is the minimal polynomial  $m_\beta(x)$  of the ONBG.

We can clearly recognize that the sequence of polynomials  $f_i(x)$  are nothing but Fibonacci polynomials [McEl]. This is a beautiful and quite useful coincidence in that, they

are very easy to generate.

Now that we have seen how to *generate* the minimal poly of a ONBG, let us see how the basic arithmetic operation of multiplication of elements expressed in terms of a optimal normal basis can be done. Based on the previous discussion regarding multiplication, we see that we need the biliner form  $c_0 = \tilde{A}\Lambda\tilde{B}^T$ . For which we need the matrix of multiplication  $\Lambda$  (it clearly depends on the particular chosen normal basis  $\Rightarrow$  it is different for different normal bases). Before that, let us see how we can construct the *matrix of transformation* 'T' from the polynomial basis  $PB = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  generated by  $\alpha \rightarrow$  root of the irreducible polynomial  $m_\alpha(x)$  used to construct the field  $GF(2^n)$  (of degree  $n$ ) to optimal normal basis  $\{\beta, \beta^2, \dots, \beta^{2^{n-1}}\}$  generated by the ONBG  $\beta$  whose minimal polynomial is  $m_\beta(x)$ .

### 3.4 Matrix of Transformation 'T'

As has been stated in the previous sections Type II ONBGs usually are primitive or have large orders. Suppose if the ONBG  $\beta$  is primitive, that is it has the multiplicative order  $2^n - 1$ , we can also use it to construct the field  $GF(2^n)$  using the  $PB = \{1, \beta, \beta^2, \dots, \beta^{n-1}\}$  generated by it. In which case we call it a primitive ONBG or PONBG for short and we can develop the matrix of transformation 'T' very easily which we will see in the following sequel. But at times, we may wish to construct the field using a different irreducible polynomial (probably primitive) which has few non zero coefficients so that arithmetic with respect to the PB generated by its root  $\alpha$  (i.e modulo that irred poly) can be efficiently done or that the particular chosen field doesn't have a PONBG, then we need to look for a general method for constructing the matrix of transformation 'T'.

Let us start with the simpler case namely the ONBG is a PONBG and its minimal polynomial is used ( $\Rightarrow$  the PB generated by it) is used to construct the field. Since the only way to construct an extension field of degree  $n$  is by taking residues modulo an irreducible polynomial of degree  $n$ , that is the elements of the extension field will be after construction in terms of the PB whose generator is some root of the chosen irreducible polynomial, we have the following procedure to build the matrix 'T':

NB generated by the PONBG  $\beta$  :

$$\{\beta, \beta^2, \dots, \beta^{2^{n-1}}\}$$

PB generated by the PONBG  $\beta$  :

$$\{1, \beta, \dots, \beta^{n-1}\}$$

$$\beta \text{ in terms of } PB = (0, 1, 0, \dots, 0)$$

$$\beta \text{ in terms of } NB = (1, 0, 0, \dots, 0)$$

We have thus

$$\begin{aligned}\beta^2 &= (0, 0, 1, 0, \dots, 0) \\ \beta^3 &= (0, 0, 0, 1, \dots, 0) \\ \beta^{n-1} &= (0, 0, 0, \dots, 0, 1)\end{aligned}$$

in terms of PB and hence, if we view any element in  $\text{GF}(2^n)$  in terms of PB, we can have PB representation of product, sum of any two elements of  $\text{GF}(2^n)$  (reduced modulo  $m_\beta(x) \rightarrow$  minimal poly of  $\beta$  as well as primitive chosen irreducible polynomial.) Therefore, we can find the transformation matrix easily by multiplication modulo  $m_\beta(x)$ .

$$\begin{bmatrix} \beta \\ \beta^2 \\ \vdots \\ \beta^{2^{n-1}} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \vdots \end{bmatrix} \begin{bmatrix} 1 \\ \beta \\ \vdots \\ \beta^{n-1} \end{bmatrix}$$

$$\Rightarrow NB = T \cdot PB$$

$$\Rightarrow PB = T^{-1} \cdot NB$$

i.e we can have PB(NB) representation of any element in NB(PB) representation, once we know or to say have constructed the matrix T. Now let us recall,

$$c_k = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \lambda_{ij}^{(k)} a_i b_j$$

$$\beta^{2^i} \beta^{2^j} = \sum_{k=0}^{n-1} \lambda_{ij}^{(k)} \beta^{2^k}; \quad \lambda_{ij}^{(k)} \in \mathbb{F}_2$$

Clearly, to get  $c_0 = \bar{A} \Lambda \bar{B}^T$  i.e to get matrix  $\Lambda$ , from the above equation we can see that we need find the NB representation of the product of the cross terms:

$$\beta^{2^i} \beta^{2^j} \quad \forall 0 \leq i, j \leq n-1 \quad (n^2 \text{ elements})$$

which will involve lot of computation using  $n$ -bit elements and  $m_\beta(x)$ . So to simplify our task and arrive at  $\Lambda = (\lambda_{ij})$ , let us define another matrix 'Q' which is related to  $\lambda$  in the following way

$$Q = (q_{ij}) \text{ where } q_{ij} = \lambda_{-j, (i-j)}$$

It is easy to see that the number of nonzero entries in the matrix  $Q$  is equal to  $C_N$ , since each element of  $Q, q_{ij}$  is equal to one element of  $\Lambda, \lambda_{ij}$ , in the above shown way. Now, observe that

$$\beta^{2^0} \beta^{2^i} = \beta_0 \beta_i = \sum_{k=0}^{n-1} c_k^{(i)} \beta_k = \sum_{k=0}^{n-1} \beta_k \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \lambda_{ij}^{(k)} a_{i+k} b_{j+k}$$

$$= \sum_{k=0}^{n-1} \lambda_{-k, l-k} \beta^{2^k} = \sum_{k=1}^{n-1} q_{lk} \beta^{2^k}$$

Thus, we see that the number of nonzero entries (namely 1's) in row  $l$  of the matrix  $Q$  is equal to the number of 1's in the NB representation of basis element  $\beta_l = \beta^{2^l}$  multiplied by  $\beta_0 = \beta^{2^0}$ . Therefore, if we compute the matrix  $Q$  which requires only  $N$  products modulo  $m_\beta(x)$  ( $\beta^{2^0} \beta^{2^l}$   $0 \leq j \leq n-1$ ), we can have  $\Lambda = (\lambda_{ij})$  by the relation  $q_{ij} = \lambda_{-i, n-j}$  (i.e between the indices). So finally, to get  $\Lambda = (\lambda_{ij})$  we adopt the following efficient procedure:

- (1) Find  $m_\beta(x)$  using the Fibonacci recursive polynomials as explained in the previous section.
- (2) Find all the products  $\beta^{2^0} \beta^{2^j}$   $0 \leq j \leq n-1$  ( $n$  products) modulo  $m_\beta(x)$ .
- (3) Express the PB representation of the above products in NB representation using the transformation matrix  $T$ .
- (4) Order all the above NB representations of  $\beta^{2^0} \beta^{2^j}$   $0 \leq j \leq n-1$  with increasing  $j$  to give the matrix  $Q = (q_{ij})$ .
- (5) Use the relation  $q_{ij} = \lambda_{-j, n-i}$  to get  $(\lambda_{ij}) = \Lambda$  from  $Q = (q_{ij})$ .
- (6) Use the so obtained  $\Lambda$  in  $c_0 = \bar{A} \Lambda \bar{B}^T$  to get the complete expansion of the bilinear form corresponding to PONB representation of  $\bar{A} = (a_0, a_1, \dots, a_{n-1})$  and  $\bar{B} = (b_0, b_1, \dots, b_{n-1})$ .

Suppose the field is constructed using a different polynomial  $m_\alpha(x)$  (i.e when ONBG is not a PONBG or that you have chosen another short irreducible polynomial for that particular  $n$  which enable us to do arithmetic in PB efficiently). Then, you have to solve  $m_\beta(x)$  in the field  $\mathbb{F}_2[x]/\langle m_\alpha(x) \rangle$  using e.g *Berlekamp's Algorithm*[Men2] and pick any root

$$\beta = \sum_{k=0}^{n-1} (\beta)_k \alpha^k \cong ((\beta)_0, (\beta)_1, \dots, (\beta)_{n-1}) \quad (\beta)_k \in \mathbb{F}_2$$

Here by solving  $m_\beta(x)$  in  $\mathbb{F}_2[x]/\langle m_\alpha(x) \rangle$  we mean, finding the roots of  $m_\beta(x)$  in  $\mathbb{F}_2[x]/\langle m_\alpha(x) \rangle$  since they (roots) are the elements of  $\mathbb{F}_2[x]/\langle m_\alpha(x) \rangle$ , we will have them in PB generated by  $\alpha$ -root of  $m_\alpha(x)$ . Now, we can build the matrix of transformation  $T$  as follows (here  $\gamma_k = (\beta)_k$ , defined above.):

$$\begin{bmatrix} \beta \\ \beta^2 \\ \vdots \\ \beta^{2^{n-1}} \end{bmatrix} = \begin{bmatrix} \gamma_0 & \gamma_1 & \cdots & \gamma_k & \cdots & \gamma_{n-1} \\ \vdots & & & & & \vdots \end{bmatrix} \begin{bmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{bmatrix}$$

Now, the procedure to get  $(\lambda_{i,j}) = \Lambda$  is same as the above procedure except that we use  $m_\alpha(x)$  i.e PB generated by  $\alpha$  instead of  $m_\beta(x)$ , PB generated by the PONBG itself.

In the next chapter, we will see a novel procedure which is very simple and easy (one that involves almost no computation) to get the bilinear form of  $c_0$  in terms of  $\{a_i\}$  and  $\{a_j\}$ .

## Chapter 4

# Gao and Vanstone Basis

In the previous chapter, we looked into how Type II ONB is constructed in a field  $\text{GF}(2^n)$  which has a ONBG . We also saw the reasons as to why we study only TypeII ONB. Now in this chapter , let us see how we can derive another basis from TypeII ONB by rearranging it in a proper well-defined ( one to one )manner[GaV]. By doing so , we will see that we can arrive at a different method for exponentiation (and hence multiplication),using which we can derive the bilinear form for  $c_0 = \bar{A}\Lambda\bar{B}^T$  very easily.

### 4.1 A New Basis

Let us recall the way TypeII ONBs are constructed:

Type II: Let  $2n + 1$  be a prime and assume that  $\mathbb{Z}_{2n+1}^*$  is generated by 2 and  $-1$ . Then  $\alpha = \gamma + \gamma^{-1}$  generates an optimal normal basis for  $\text{GF}(2^n)$  where  $\gamma$  is a  $(2n + 1)$  st root of unity.

Therefore the optimal normal basis generated by  $\alpha$  is  $\{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\}$ . We will arrange the elements of the basis in a different order. For an integer  $i$  , define  $\gamma_i = \gamma^i + \gamma^{-i} = \gamma_{-i}$ . Obviously  $\gamma_0 = 0$  and  $\gamma_1 = \alpha$ . As the multiplicative order of  $\gamma$  is  $2n + 1$ , it is easy to check that  $\gamma_i = \gamma_j$  iff  $i \equiv \pm j \pmod{2n + 1}$ . So  $\gamma_1, \gamma_2, \dots, \gamma_n$  are the distinct nonzero  $\gamma_i$ 's. We can claim that

$$\{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\} = \{\gamma_1, \gamma_2, \dots, \gamma_n\}.$$

The reason is that for each  $0 \leq i \leq n - 1$ ,  $\alpha^{2^i} = \gamma^{2^i} + \gamma^{-2^i} = \gamma_{2^i}$  belongs to the set of the right-hand side, while for each  $1 \leq i \leq n$ , since  $\mathbb{Z}_{2n+1}^*$  is generated by 2 and  $-1$ , there is an integer  $k$  such that  $i \equiv \pm 2^k \pmod{2n + 1}$ , and thus  $\gamma_i = \alpha^{2^k}$  belongs to the set of the left-hand side .

Therefore,  $\gamma_1, \gamma_2, \dots, \gamma_n$  form a basis of  $\text{GF}(2^n)$  over  $\text{GF}(2)$ . To facilitate multiplication of elements represented under this basis ,we define a new function from the set of integers to the set  $\{0, 1, \dots, n\}$ . For any integer  $i$ , define  $s(i)$  to be the unique integer such that

$$0 \leq s(i) \leq n, i \equiv s(i) \pmod{2n+1} \text{ or } i \equiv -s(i) \pmod{2n+1}.$$

Obviously,  $s(0) = 0, s(i) = s(-i)$  and

$$\gamma_i = \gamma_{s(i)}, \alpha^{2^i} = \gamma_{s(2^i)} \quad \forall i.$$

As  $\gamma_i \cdot \gamma_j = \gamma_{i-j} + \gamma_{i+j}$  for all  $i, j$ , we have

$$\gamma_i \cdot \gamma_j = \gamma_{s(i+j)} + \gamma_{s(i-j)}, \quad 1 \leq i, j \leq n.$$

Next we show how to compute the product  $\gamma_i \cdot A$ , where  $1 \leq i \leq n$  and  $A$  is an arbitrary element in  $\text{GF}(2^n)$ . Suppose that  $A = \sum_{k=1}^n a_k \gamma_k$ , where  $a_k \in \text{GF}(2)$ . Then

$$\gamma_i \cdot A = \sum_{k=1}^n a_k \gamma_i \cdot \gamma_k = \sum_{k=1}^n a_k (\gamma_{s(k+i)} + \gamma_{s(k-i)}).$$

Note that

$$\begin{aligned} \sum_{k=1}^n a_k \gamma_{s(k+i)} &= \sum_{k=1}^{n-i} a_k \gamma_{k+i} + \sum_{k=n+1-i}^n a_k \gamma_{2n+1-(k+i)} \\ &= \sum_{k=i+1}^n a_{k-i} \gamma_k + \sum_{k=n+1-i}^n a_{2n+1-(k+i)} \gamma_k \\ &= \sum_{k=i+1}^n a_{s(k-i)} \gamma_k + \sum_{k=n+1-i}^n a_{s(k+i)} \gamma_k, \\ \sum_{k=1}^n a_k \gamma_{s(k-i)} &= \sum_{k=1}^i a_k \gamma_{i-k} + \sum_{k=i+1}^n a_k \gamma_{k-i} \\ &= \sum_{k=1}^i a_{i-k} \gamma_k + \sum_{k=1}^{n-i} a_{k+i} \gamma_k \\ &= \sum_{k=1}^i a_{s(k-i)} \gamma_k + \sum_{k=1}^{n-i} a_{s(k+i)} \gamma_k, \end{aligned}$$

where here, and hereafter, we assume that  $a_0 = 0$ . We see that

$$\begin{aligned} \gamma_i \cdot A &= \sum_{k=1}^n (a_{s(k-i)} + a_{s(k+i)}) \gamma_k \\ &= \sum_{k=1}^c (a_{i-k} + a_{k+i}) \gamma_k + \sum_{k=c+1}^d f(k) \gamma_k + \sum_{k=d+1}^n (a_{k-i} + a_{2n+1-(k+i)}) \gamma_k, \end{aligned}$$



where  $c = \min(i, n - i)$ ,  $d = \max(i, n - i) = n - c$  and

$$f(k) = \begin{cases} a_{i-k} + a_{2n+1-(k+i)} & \text{if } i > n - i \\ a_{k-i} + a_{k+i} & \text{if } i < n - i \end{cases}$$

This shows that  $\gamma_i \cdot A$  can be computed in  $O(n)$  bit operations.

Now, to compute  $\alpha^e$  we can assume that  $0 \leq e \leq 2^n - 1$ , as  $\alpha^{2^n-1} = 1$ . Write  $e = \sum_{k=0}^{n-1} e_k 2^k$ , where  $e_k \in \{0, 1\}$ . Then

$$\alpha^e = \prod_{k=0}^{n-1} (\alpha^{2^k})^{e_k} = \prod_{k=0}^{n-1} (\gamma_{s(2^k)})^{e_k}.$$

This suggests that  $\alpha^e$  can be computed iteratively as follows:

**Algorithm:**

**Input:** An integer  $e$  with  $0 \leq e \leq 2^n - 1$ .

**Output:**  $\alpha^e$  represented in the basis  $(\gamma_1, \gamma_2, \dots, \gamma_n)$

**Step1:** Set  $A := 1 = \sum_{k=1}^n \gamma_k$  and compute the binary representation:  $e = \sum_{k=0}^{n-1} e_k 2^k$ ;

**Step2:** For  $k$  from 0 to  $n - 1$ , if  $e_k = 1$  then set  $A := \gamma_{s(2^k)} \cdot A$ ;

**Step3:** Return  $A$ ;

**End.**

The correctness of the algorithm is obvious. The major cost is incurred at Step 2 where  $v(e)$  products of the form  $\gamma_i \cdot A$  are computed. Since we have shown that each such product can be computed in  $O(n)$  bit operations, the total cost is  $O(n \cdot v(e))$  bit operations. Therefore,  $\alpha^e$  can be computed in  $O(n \cdot v(e))$  bit operations.

Now, multiplication in terms of the above *Gao and Vanstone basis* can be accomplished in the following obvious way:

$$C = A \cdot B = \sum_{k=1}^n a_k (\gamma_k \cdot B)$$

where  $(\gamma_k \cdot B)$  is given by the expression we derived before looking into exponentiation algorithm. Using the above described form of multiplication let us see how we can derive the bilinear form for  $c_0$  (in terms of the coordinates of  $A$  and  $B$  with respect to optimal normal basis  $\{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\}$ ) in the next section.

## 4.2 Bilinear Form Derived

Let us define the coordinate vectors of elements of the field  $\text{GF}(2^n)$  (again here we assume that the existence of an Type II ONBG in this field has been verified) with respect to  $\text{ONB} = \{\alpha, \alpha^2, \dots, \alpha^{2^{n-1}}\}$  and the above introduced Gao and Vanstone basis  $= \{\gamma_1, \gamma_2, \dots, \gamma_n\}$  as follows:

$$A = \sum_{k=1}^n a'_k \gamma_k = \sum_{k=0}^{n-1} a_k \alpha^{2^k}$$

That is

$$A \equiv (a'_1, a'_2, \dots, a'_n) \rightarrow \{\gamma_k\} \text{ basis}$$

$$A \equiv (a_0, a_1, \dots, a_{n-1}) \rightarrow \{\alpha^{2^k}\} \text{ basis}$$

The main observation which we will use here is that Gao and Vanstone basis  $\{\gamma_k\}$  is obtained from Type II ONB  $\{\alpha^{2^k}\}$  by permuting in a one-to-one well defined manner. The permutation is given by  $(2^k \rightarrow s(2^k))$  That is (recall the definition of  $s(i)$ , from the previous section)

$$2^k \equiv \pm i \pmod{2n+1} \quad 1 \leq i \leq n.$$

$$\text{maps } \alpha^{2^k} = \gamma_{2^k} \text{ to } \gamma_{s(2^k)} = \gamma_i \quad \forall i$$

(since  $\gamma$  is a  $(2n+1)$  'st root of unity). This implies that, given an element  $A$  :

$$A \equiv (a'_1, a'_2, \dots, a'_n) \rightarrow \{\gamma_k\}$$

$$A \equiv (a_0, a_1, \dots, a_{n-1}) \rightarrow \{\alpha^{2^k}\}$$

each  $a_i$  is mapped to a unique  $a'_j = a'_{s(2^i)}$  by the map  $i \rightarrow 2^i \leftrightarrow s(2^i)$ .

Now let

$$C = A \cdot B = \sum_{i=1}^n a'_i (\gamma_i \cdot B) = \sum_{k=1}^n c'_k \gamma_k = \sum_{k=0}^{n-1} c_k \alpha^{2^k}$$

$$c_k = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j \lambda_{ij}^{(k)}$$

$$C \equiv (c'_1, c'_2, \dots, c'_n)$$

$$C \equiv (c_0, c_1, \dots, c_{n-1})$$

Since  $\gamma_1 = \alpha_{2^0} = \gamma_{s(2^0)}$ ;  $c'_1 = c_0$ . (Remember that we have assumed that  $b'_0 = 0$  in the expansion of  $(\gamma_i \cdot B)$  Therefore we have on comparing the coefficients of  $c'_1$  on both sides of the product equation given above (i.e with  $i = 1$ ):

$$c'_1 = c_0 = a'_1(b'_{1-1} + b'_{1+1}) + a'_2(b'_{2-1} + b'_{2+1}) + \dots + a'_n(b'_{(.)-} + b'_{(.)+})$$

$$c'_1 = c_0 = a'_1(b'_0 + b'_2) + a'_2(b'_1 + b'_3) + \dots$$

Now since we have the one-to-one correspondence  $a_k \leftrightarrow a'_{s(2^k)}$  (similarly for  $b_k$ 's) given by computing the pairs  $(2^k, s(2^k))$  we can write the above expression for  $c'_1 = c_0$  entirely in terms of  $a_k$ 's and  $b_k$ 's which is what we want, namely the bilinear form for  $c_0$ . in terms of coordinates w.r.t ONB generated by  $\alpha$  of  $A$  and  $B$ . Upon summarizing the method we have the following procedure:

- (1) Compute the correspondence pairs  $(2^k, s(2^k)) 0 \leq k \leq n$
- (2) Substitute  $i = 1$  in the expansion of  $(\gamma_i \cdot B)$  to get the expression for  $c'_1 = c_0$  in terms of  $a'_k$ 's and  $b'_k$ 's.
- (3) De-associate using the computed correspondence pairs to get the bilinear form for  $c_0$ .

Observe that since  $b'_0 = 0$  we have  $2(n-1)$  forms of the type  $a_i b_j, i \neq 0$  and the term  $a_0 b_1$  so in total we have  $2(n-1) + 1 = 2n - 1$  forms. This is what is expected, since we are working with optimal normal bases which have complexity  $C_N = 2n - 1$ . Moreover this method gives directly the expression in the form of sum of  $(2n - 1)$  forms of the type  $a_i(b_j + b_k)$  which is efficiently implementable in software or hardware. We can easily verify that it is commutative  $\Rightarrow C = A \cdot B = B \cdot A$ .

## Chapter 5

# Design and Implementation

In this chapter we will first see how to do certain computations efficiently. The computations which we will be interested mostly are those related to the efficient implementation of Elliptic Curve Cryptosystems. Here we will confine our attention only to curves over finite fields. In the later sections we will see the design aspects involved.

### 5.1 Certain Computations

In this section we will see how we can solve the equation of the elliptic curve over finite fields (of nonzero characteristic) given in Weierstrass affine (non-homogeneous form) form. Firstly let us consider curves over  $\text{GF}(2^n)$ . Since it is clear from our previous chapters, we will be working entirely with those extensions of  $\text{GF}(2)$  which have an ONBG in them and hence we assume that the elements of the field are expressed w.r.t the normal basis generated by the ONBG and that multiplication of field elements is done using the bilinear form for  $c_0$ . We will see in this section some more advantages of expressing the elements of the field in terms of a normal basis.

Let us recall the Weierstrass equation for an elliptic curve using non-homogeneous (affine) coordinates  $x = X/Z, y = Y/Z$ :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

An Elliptic curve  $E$  is the set of solutions to the above equation in  $\bar{K} * \bar{K}$  (where  $\bar{K}$  is the algebraic closure of the field  $K$  over which the curve is defined), together with the extra point at infinity  $\mathcal{O}$ . If  $a_1, a_2, a_3, a_4, a_6 \in K$ , then  $E$  is said to be *defined over  $K$* , and we denote this by  $E/K$ . If  $E$  is defined over  $K$ , then the set of  $K$ -rational points of  $E$ , denoted by  $E(K)$ , is the set of points both of whose coordinates lie in  $K$ , together with the point  $\mathcal{O}$ .

**Solving for the  $K$ -rational points of  $E$  i.e  $E(K)$  where  $K = \text{GF}(2^m)$ :**

The Weierstrass eqn can be written as follows

$$y^2 + (a_1x + a_3)y = (x^3 + a_2x^2 + a_4x + a_6)$$

$$\Rightarrow y^2 + B(x)y = C(x)$$

where  $B(x) = (a_1x + a_3)$ ,  $C(x) = [x^2(x + a_2) + (a_4x + a_6)]$  Therefore, solving for the  $K$ -rational points of  $E$  involves the solution of the above quadratic eqn for all  $x \in \text{GF}(2^m) = K$ .

Let  $\beta$  be the NBG i.e  $\text{NB} = \{\beta^{2^0}, \beta^{2^1}, \dots, \beta^{2^{m-1}}\}$ . Clearly  $\beta^2, \beta^{2^2}, \dots$  are the conjugates of  $\beta$ . Let  $a \in \text{GF}(2^m)$ . Then

$$a = \sum_{i=0}^{m-1} a_i \beta^{2^i} \text{ where } a_i \in \mathbb{F}_2$$

Now, we have the *Trace* function  $\text{Tr}(\cdot)$  given by:

$$\text{Tr} : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$$

$$\text{Tr}(a) = \sum_{i=0}^{m-1} a^{2^i} \text{ for any } a \in \mathbb{F}_{2^m}$$

Since Trace is a *surjective homomorphism* and that  $\ker(\text{Tr}) \neq \mathbb{F}_{2^m}$  (i.e is a strict subset of  $\text{GF}(2^m)$ ), we have that half of the elements ( $2^{m-1}$ ) will have  $\text{Trace} = 1$  and half with  $\text{Trace} = 0$ . (since  $|\ker| \cdot |\text{image}| = |G|$  for any group  $G$  and that in our case,  $|\text{image}| = 2$ ). We also have the following obvious properties of Trace:

$$\text{Tr}(a\alpha + b\beta) = a\text{Tr}(\alpha) + b\text{Tr}(\beta) \forall a, b \in \mathbb{F}_2 \text{ and } \alpha, \beta \in \mathbb{F}_{2^m}$$

$$\text{Tr}(a^{2^i}) = \text{Tr}(a) \text{ i.e of conjugates of } a$$

Therefore we have:

$$\text{Tr}(a) = \sum_{i=0}^{m-1} a_i \text{Tr}(\beta^{2^i}) = \sum_{i=0}^{m-1} a_i \text{Tr}(\beta)$$

$$\text{Tr}(a) = \left( \sum_{i=0}^{m-1} a_i \right) \text{Tr}(\beta) \text{ for some } a \in \mathbb{F}_{2^m}$$

Clearly from the above equation the Trace of a normal basis generator has to be 1, or else it would imply that the Trace of every element is 0. Hence we conclude that:

$$\text{Tr}(\beta) = 1 \text{ if } \beta \text{ is a normal basis generator}$$

And hence

$$\text{Tr}(\beta) = (\beta + \beta^{2^1} + \beta^{2^2} + \dots + \beta^{2^{m-1}}) = 1$$

$$\Rightarrow \text{the element } 1 \equiv (1, 1, 1, \dots, 1, 1)$$

i.e vector of all 1's w.r.t a NB. We thus have that the *Trace of any element in terms of a NB representation is simply given by the sum of its coordinates*. Now let us turn to the problem of solving the quadratic

$$y^2 + By = C$$

(Here  $B$  and  $C$  mean  $B(x)$  and  $C(x)$  i.e the  $x$  dependency is understood from the previous section) We will study the following different cases:

CASE 1: When  $B = 0, C \neq 0$ :

$$\Rightarrow y^2 = C = \gamma \text{ (say)}$$

for which we clearly have the unique solution:

$$y = \gamma^{2^{n-1}}$$

which involves 1 left shift ( $\Rightarrow n - 1$  right shifts).

CASE 2:  $B = 1, C \neq 0$ )

$$\Rightarrow y^2 + y = C = \gamma$$

which has solutions iff  $Tr(\gamma) = 0$ . Now let  $\gamma = (\gamma_0, \gamma_1, \dots, \gamma_{m-1})$  in terms of the chosen NB. Let

$$\begin{aligned} y &= (y_0, y_1, \dots, y_{m-1}) \\ \Rightarrow y^2 &= (y_{m-1}, y_0, \dots, y_{m-2}) \end{aligned}$$

Therefore

$$y^2 + y = \gamma \Rightarrow$$

$$y_0 + y_{m-1} = \gamma_0,$$

$$y_0 + y_1 = \gamma_1,$$

$$y_1 + y_2 = \gamma_2,$$

and so on, by comparing the coordinate vectors on both sides. Clearly, fixing  $y_0 = 0$  gives one solution and  $y_0 = 1$  gives the other solution of the quadratic uniquely, since all other  $y_i$ 's can be solved for.

CASE 3:  $B \neq 0, C \neq 0$ :

$$\Rightarrow y^2 + By = C$$

Set  $z = B^{-1}y$   $\gamma = C(B^{-1})^2$  then the above equation reduces to CASE 2:

$$\Rightarrow z^2 + z = \gamma$$

which has solutions iff  $Tr(\gamma) = Tr(C(B^{-1})^2) = 0$  and the solutions of the original equation are given by

$$y_1 = Bz_1 \quad y_2 = B(z_1 + 1) = Bz_2$$

Now let us see how we can compute the inverse of an element efficiently. The most efficient technique, from the point of view of minimizing the number of multiplications, to compute an inverse of an element of  $GF(2^m)$  was proposed by Itoh, Teichai, and Tsuji[Men1]. Observe that if  $\alpha \in \mathbb{F}_{2^m}, \alpha \neq 0$ , then

$$\alpha^{-1} = \alpha^{2^m-2} = (\alpha^{2^{m-1}})^2$$

If  $m$  is odd, then since

$$2^{m-1} - 1 = (2^{(m-1)/2} - 1)(2^{(m-1)/2} + 1)$$

we have

$$\alpha^{2^{m-1}-1} = (\alpha^{2^{(m-1)/2}-1})^{(2^{(m-1)/2}+1)}$$

Hence it takes only one multiplication to evaluate  $\alpha^{(2^{m-1}-1)}$  once the quantity  $\alpha^{(2^{(m-1)/2}-1)}$  has been computed (we are ignoring the cost of squaring). If  $m$  is even, then we have

$$\alpha^{2^m-1} = \alpha^{2(2^{(m-2)/2}-1)(2^{(m-2)/2}+1)+1}$$

and consequently it takes two multiplications to evaluate  $\alpha^{2^m-1}$  once  $\alpha^{(2^{(m-2)/2}-1)}$  has been computed. The procedure is then repeated recursively.

Now let us consider solving a curve (quadratic in  $y$ ) defined over  $\mathbb{F}_p$ . Curves over such fields can be reduced to the Weierstrass short normal form:

$$y^2 = x^3 + ax + b$$

Therefore a curve can be described by the coefficients  $(a, b)$ . For a given  $x$ , solving the curve means solving the quadratic  $y^2 = x^3 + ax + b = c$  over  $\mathbb{F}_p$ . So let us how to compute square roots modulo  $p$ : We know that the quadratic congruence  $x^2 = a \pmod p$  has solutions iff the Legendre Character (or symbol)  $\lambda_p(a)$  [Ono] [Chah] [IrRo] (This is analogous to the Trace function in the  $GF(2^m)$  case)  $\lambda_p(a) \equiv a^{(p-1)/2} \pmod p \equiv 1 \pmod p$  [Ono][IrRo]. Using quadratic reciprocity (or using  $a^{(p-1)/2} \equiv \pmod p$ ), one can quickly determine whether or not

an integer  $a$  is a quadratic residue modulo  $p$ . However, if it is a residue, that does not tell us how to find a solution to the congruence  $x^2 \equiv a \pmod{p}$  — it tells us only that a solution exists. Let us see an (efficient) algorithm for finding a square root of a residue  $a$  once we know any nonresidue  $n$ .

Let  $p$  be an odd prime, and suppose that we somehow know a quadratic nonresidue  $n$ . Let  $a$  be an integer such that  $\lambda_p(x) = 1$ . We want to find an integer  $x$  such that  $x^2 \equiv a \pmod{p}$ . Here is how we proceed. First write  $p - 1$  in the form  $2^\alpha \cdot s$ , where  $s$  is odd. Then compute  $n^s$  modulo  $p$ , and call that  $b$ . Next compute  $a^{(s+1)/2}$  modulo  $p$ , and call that  $r$ . Our first claim is that  $r$  comes reasonably close to being a square root of  $a$ . More precisely, if we take the ratio that  $r^2$  to  $a$ , we claim that we get a  $2^\alpha - 1$  th root of unity modulo  $p$ . Namely, we compute (for brevity, we shall use the equality to mean congruence modulo  $p$ , and we use  $a^{-1}$  to mean the inverse of  $a$  modulo  $p$ ):

$$(a^{-1}r^2)^{2^\alpha-1} = a^{(p-1)/2} = \lambda_p(x) = 1.$$

We must then modify  $r$  by a suitable  $2^\alpha$  th root of unity to get an  $x$  such that  $x^2/a$  is 1. To do this, we claim that  $b$  is a *primitive*  $2^\alpha$  th root of unity, which means that all  $2^\alpha$  th roots of unity are powers of  $b$ . To see this, first we note that  $b$  is a  $2^\alpha$  th root of 1, because  $b^{2^\alpha} = n^{2^\alpha s} = n^{p-1} = 1$ . If  $b$  were't primitive, there would be a lower power (a divisor of  $2^\alpha$ ) of  $b$  that gives 1. But then  $b$  would be an even power of a primitive  $2^\alpha$  th root of unity, and so would be a square in  $\mathbb{F}_p^*$ . This is impossible, because  $\lambda_p(b) = [\lambda_p(n)]^s = -1$  (since  $s$  is odd and  $n$  is a nonresidue). Thus,  $b$  is a primitive  $2^\alpha$  th root of unity. So it remains to find a suitable power  $b^j$   $0 \leq j < 2^\alpha$ , such that  $x = b^j r$  gives the desired square root of  $a$ . To do that, we write  $j$  in binary as  $j = j_0 + 2j_1 + 4j_2 + \cdots + 2^{\alpha-2}j_{\alpha-2}$ , and show how one successively determines whether  $j_0, j_1, \dots$  is 0 or 1. (Note that, we may suppose that  $j < 2^{\alpha-1}$ , since  $b^{2^{\alpha-1}} = -1$ , and so  $j$  can be modified by  $2^{\alpha-1}$  to give another  $j$  for which  $b^j r$  is the other squareroot of  $a$ .) Here is the inductive procedure for determining the binary digits of  $j$ :

- (1). Raise  $(r^2/a)$  to the  $2^{\alpha-2}$  th power. We proved that the square of this is 1. Hence, you get either  $\pm 1$ . If you get 1, take  $j_0 = 0$ ; if you get  $-1$ , take  $j_0 = 1$ . Notice that  $j_0$  has been chosen so that  $((b^{j_0}r)^2/a)$  is a  $2^{\alpha-2}$  th root of unity.
- (2). Suppose you've found  $j_0, \dots, j_{k-1}$  such that  $(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}}r)^2/a$  is a  $2^{\alpha-k-1}$  th root of unity, and you want  $j_k$ . Raise this number to half the power that gives 1, and choose  $j_k$  according to whether you get  $+1$  or  $-1$ :

$$\text{if } ((b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}}r)^2/a)^{2^{\alpha-k-2}} = 1 \text{ or } -1$$

then take  $j_k = 0$  or  $1$  respectively.



We easily check that with this choice of  $j_k$  the "corrected" value comes closer to being a square root of  $a$ , i.e., we find that  $(b^{j_0+2j_1+\dots+2^{k-1}j_{k-1}}r)^2/a$  is a  $2^{\alpha-k-2}$  th root of unity.

When we get to  $k = \alpha - 2$  and find  $j_{\alpha-2}$ , we then have

$$(b^{j_0+2j_1+\dots+2^{\alpha-2}j_{\alpha-2}}r)^2/a = 1,$$

i.e.  $b'r$  is a square root of  $a$ , as desired.

**Remarks.** 1. The easiest case of this algorithm occurs when  $p$  is a prime which is  $\equiv 3 \pmod{4}$ . Then  $\alpha = 1, s = (p-1)/2$ , so  $(s+1)/2 = (p+1)/4$ . and we see that  $x = r = a^{(p+1)/4}$  is already the desired square root.

2. We now discuss the time estimate for this algorithm. We suppose that we start already knowing the information that  $n$  is a nonresidue. The steps in finding  $s, b$  and  $r = a^{(s-1)/2}$  (working modulo  $p$ , of course) take at most  $O(\log^3 p)$  bit operations. Then in finding  $j$  the most time-consuming part of the  $k$ -th induction step is raising a number to the  $2^{\alpha-k-2}$  th power, and this means  $\alpha - k - 2$  squarings mod  $p$  of integers less than  $p$ . Since  $\alpha - k - 2 < \alpha$ , we have the estimate  $O(\alpha \log^2 p)$  for each step. Thus, since there are  $\alpha - 1$  steps, the final estimate is  $O(\log^3 p + \alpha^2 \log^2 p) = O(\log^2 p (\log p + \alpha^2))$ . At worst (if almost all of  $p - 1$  is a power of 2), this is  $O(\log^4 p)$ , since  $\alpha < \log_2 p = O(\log p)$ . Thus, given a nonresidue modulo  $p$ , we can extract square roots mod  $p$  in polynomial time (bounded by the fourth power of the number of bits in  $p$ ).

3. Strictly speaking, it is not known (unless one assumes the validity of the so called "Riemann Hypothesis") whether there is an algorithm for finding a nonresidue modulo  $p$  in polynomial time. However, given any  $\epsilon > 0$  there is a polynomial time algorithm that finds a nonresidue with a probability greater than  $1 - \epsilon$ . Namely, a randomly chosen number  $n, 0 \leq n \leq p$ , has a 50% chance of being a nonresidue, and this can be checked in polynomial time. If we do this for  $\log_2(1/\epsilon)$  different randomly chosen  $n$ , then with a probability  $> 1 - \epsilon$  at one of them will be a nonresidue.

We have till now looked into how we can solve a quadratic over finite fields of characteristic 2 or  $p$ . Now let us see where we will be using them in the context of *Elliptic Curve Cryptosystems(ECC)* [Men1].

Irrespective of the scheme we use to implement ECC (e.g. El Gamal, Omura-Massey [Kob1]), we have to implement one important common (to all) essential aspect, namely **message embedding**. That is, we will have to first embed the message onto some point on the (chosen) elliptic curve before going to the actual scheme. So let us see how we can embed a message onto a point on the elliptic curve. Here is one possible probabilistic method to imbed plaintexts as points on an elliptic curve  $E$  defined over  $\text{GF}(q)$ , where  $q = p^r$  is assumed to be large (and odd). Let  $k$  be a large enough integer so that we are satisfied with a failure probability of 1 out of  $2^k$  when we attempt to imbed a plaintext

message units  $m$ ; in practice  $k = 30$  or at worst  $k = 50$  should suffice. We suppose that our message units  $m$  are integers  $0 \leq m \leq M$ . We also suppose that our finite field is chosen so that  $q > Mk$ . We write the integers from 1 to  $Mk$  in the form  $mk + j$ , where  $1 \leq j \leq k$ , and we set up 1-to-1 correspondence between such integers and a set of elements  $\text{GF}(q)$ . For example, we write such an integer as an  $r$ -digit integer to the base  $p$ , and take the  $r$  digits, considered as elements of  $\mathbb{Z}/p\mathbb{Z}$ , as the coefficients of a polynomial of degree  $r - 1$  corresponding to an element of  $\mathbb{F}_q$ . That is, the integer  $(a_{r-1}, a_{r-2}, \dots, a_0)_p$  corresponds to the polynomial  $\sum_{i=0}^{r-1} a_i X^i$ , which, considered modulo some degree- $r$  irreducible polynomial over  $\mathbb{F}_p$ , gives an element of  $\mathbb{F}_q$ . We can apply the above method even to curves over  $\text{GF}(2^m)$ .

Thus, given  $m$ , for each  $j = 1, 2, \dots, k$  we obtain an element  $x$  of  $\mathbb{F}_q$  corresponding to  $mk + j$ . For such an  $x$ , we compute the right side of the equation

$$y^2 = f(x) = x^3 + ax + b$$

and try to find a square root of  $f(x)$  using the method explained above. (Although the algorithm was given for the prime field  $\mathbb{F}_p$ , it carries over to any finite field  $\mathbb{F}_q$ . In order to use it we must have a nonsquare  $g$  in the field, which can easily be found by a probabilistic algorithm.) If we find a  $y$  such that  $y^2 = f(x)$ , we take  $P_m = (x, y)$ . If it turns out that  $f(x)$  is nonsquare, then we increment  $x$  by 1 and try again. Provided we find an  $x$  for which  $f(x)$  is a square before  $j$  gets bigger than  $k$ , we can recover  $m$  from the point  $(x, y)$  by the formula  $m = \lfloor (\tilde{x} - 1)/k \rfloor$ , where  $\tilde{x}$  is the integer corresponding to  $x$  under 1-to-1 correspondence between integers and elements of  $\mathbb{F}_q$ . Since  $f(x)$  is a square for approximately 50% of all  $x$ , there is only about a  $2^{-k}$  probability that this method will fail to produce a point  $P_m$  whose  $x$ -coordinate corresponds to an integer  $\tilde{x}$  between  $mk + 1$  and  $mk + k$ . (More precisely, the probability that  $f(x)$  is a square is essentially equal to  $N/2q$ ; but  $N/2q$  is very close to  $1/2$ .)

## 5.2 Construction of Elliptic Curves

Let us recall certain basic properties of quadratic forms and fields that are necessary for the following sections. We will first see quadratic forms, that are easy to compute with, and then quadratic fields (imaginary) that are well suited for explaining the theory. *These are two sides of the same object.*

### Quadratic Forms:

The following results are well known and can be found in [Rose][Jones][Chah][Cohn1]. Let  $\delta = -D$  be a fundamental discriminant, i.e.,  $D$  is a positive integer which is not divisible by any square of an odd prime and which satisfies  $D \equiv 3 \pmod{4}$  or  $D \equiv 4, 8 \pmod{16}$ .

A *quadratic form* of discriminant  $-D$  is a 3-tuple of integers  $(a, b, c)$  such that  $b^2 - 4ac = \delta = -D$ . There is a correspondence between the set of quadratic forms and the set of  $2 \times 2$  matrices with half integer coefficients. With  $Q = (a, b, c)$ , we associate the  $2 \times 2$  matrix

$$M(Q) = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

Two forms  $Q$  and  $Q'$  of the same discriminant are said to be *equivalent* (or  $Q \sim Q'$ ) if there exists  $N$  in  $SL_2(\mathbb{Z})$  (i.e., a  $2 \times 2$  integer matrix with determinant 1) such that

$$M(Q') = N^{-1}M(Q)N$$

This clearly defines an equivalence relation on the quadratic forms. It can be shown that **Prop**: Each equivalence class contains exactly one form  $(a, b, c)$  with  $a, b, c$  relatively prime and satisfying  $|b| \leq a \leq c$  and  $(|b| = a, \text{ or } a = c \Rightarrow b > 0)$ . Such a form is called *reduced*.

There is a algorithm to compute a reduced form to a given equivalent form: refer [AtMo].

The set of primitive reduced quadratic forms of discriminant  $\delta = -D$ , denoted by  $\mathcal{C}(-D) = \mathcal{C}(\delta)$ , is finite (for  $|b| \leq \sqrt{D/3}$  if  $(a, b, c)$  is reduced). Moreover, it is possible to define an operation on classes that gives to  $\mathcal{C}(\delta)$  the structure of an Abelian group. This operation is called the *composition of classes* and is ordinarily written multiplicatively [Cohn2]. For the actual computation, see [AtMo]. The order of  $\mathcal{C}(-D)$  is denoted by  $h(-D) = h(\delta)$ . The neutral element  $F_D$  is called the *principal form*. It is equal to  $(1, 0, D/4)$  or  $(1, 1, (D+1)/4)$  according as  $D \equiv 0$  or  $3 \pmod{4}$ .

### Quadratic fields:

Consider now  $K = \mathbb{Q}(\sqrt{-D})$ . The extension  $K/\mathbb{Q}$  is Abelian of degree 2, of Galois group  $\{1, *\}$ , where  $*$  denotes complex conjugation. The ring of integers of  $K$  is  $\mathcal{O}_K = \mathbb{Z}[\omega]$ , where

$$\omega = \begin{cases} \sqrt{-D/4} & \text{if } D \equiv 0 \pmod{4} \\ \frac{1+\sqrt{-D}}{2} & \text{otherwise.} \end{cases}$$

The conjugate of an element  $\alpha = x + y\omega$  is  $\alpha' = \alpha^* = x + y\omega^*$ . The Trace (resp. norm) of  $\alpha$  is  $Tr(\alpha) = \alpha + \alpha^*$  (resp.  $N_K(\alpha) = \alpha(\alpha^*)$ ). If  $\alpha$  is an element of  $K$ , its *associates* are the  $v\alpha$ , where  $v$  is any unit of  $K$  (that is,  $N_K(\alpha) = 1$ ). The number of units is denoted by  $w(-D)$  and is equal to 6, 4, or 2 according to  $D$  equal to 3, 4, or  $> 4$ . The group of units is denoted by  $\mathcal{O}_K^\times$ .

The decomposition of the ideal  $(p)$  in  $K$  is given by the following theorem:

**Prop**: If  $(-D/p) = +1$ , the ideal  $(p)$  splits as the product of two distinct ideals in  $K$ . If  $(-D/p) = 0$ ,  $p$  ramifies, and if  $(-D/p) = -1$ , it is inert.

We have an useful result:

**Prop :** The equation  $p = N_K(\pi)$  has a solution in  $\mathcal{O}_K$  iff splits as the product of two principal ideals in  $K$ . This is equivalent to saying that  $p$  is represented by the principal form of discriminant  $-D$ . In other words:  $4p = A^2 + DB^2$  with  $A$  and  $B$  in  $\mathbb{Z}$ .

If  $p$  is representable by the principal form of discriminant  $-D$ , we shall say that  $p$  is a norm in  $\mathbb{Q}(\sqrt{-D})$  or simply  $p$  is a norm when the context is clear. Conversely, we shall say that  $-D$  is good for  $p$  if  $p$  is a norm. Thus, in general,  $(-D/p) = 1$ , that  $p$  splits in  $\mathbb{Q}(\sqrt{-D})$ , even that  $p$  is representable by a form of the principal genus, are all necessary conditions for  $p$  to be a norm.

### Ideal Classes and Quadratic Forms:

The class group of an order  $\mathcal{O}$  in  $K$  (i.e. the group of invertible fractional  $\mathcal{O}$  ideals), its class number and discriminant will be denoted by  $\mathcal{CL}(\mathcal{O})$ ,  $h(\mathcal{O})$  and  $\delta(\mathcal{O})$ , respectively. In the special case in which  $\mathcal{O} = \mathcal{O}_K$  is the maximal order of  $K$  we shall use the abbreviating notations  $\mathcal{C}_K = \mathcal{CL}(\mathcal{O}_K)$ ,  $h_K = h(\mathcal{O}_K)$  and  $\delta_K = \delta(\mathcal{O}_K)$ . Ideal classes of  $\mathcal{O}$  will be represented by  $SL_2(\mathbb{Z})$ -equivalence classes  $[Q]$  of (in our context positive definite binary) quadratic forms  $Q = (a, b, c)$  of discriminant  $\delta(\mathcal{O}) = b^2 - 4ac$ . To each quadratic form we associate the number  $\tau_Q = (-b + \sqrt{\delta}/2a)$  which is the unique root of  $Q(\tau, 1) = a\tau^2 + b\tau + c$  lying in the upper half plane  $\mathbb{H}$ . We have the following connection between ideal classes and quadratic forms [Heck] [Cohn1] [Cohn2]:

**Theorem :** Let  $\mathcal{O}$  be the order of discriminant  $\delta$  in the imaginary quadratic field  $K = \mathbb{Q}(\sqrt{\delta})$ .

- (1). If  $Q = (a, b, c) : (x, y) \rightarrow ax^2 + bxy + cy^2$  with  $a, b, c \in \mathbb{Z}$  is a quadratic form of discriminant  $\delta$ , then  $[1, \tau_Q]$  is an invertible fractional  $\mathcal{O}$ -ideal.
- (2). The map sending  $Q$  to  $[1, \tau_Q]$  induces an isomorphism between the form class group  $\mathcal{C}(\delta)$  of all quadratic forms of discriminant  $\delta$  and the ideal class group  $\mathcal{CL}(\mathcal{O})$ .

### Complex Multiplication for lattices:

Let  $\Lambda = \Lambda(1, \omega) = \Lambda_\omega$  be a lattice in  $\mathbb{C}$ . Put  $M(\Lambda) = \{\alpha \in \mathbb{C}, \alpha\Lambda \subset \Lambda\}$ . It is clear that  $\mathbb{Z} \subset M(\Lambda)$ . When  $M(\Lambda)$  is greater than  $\mathbb{Z}$ , we say that  $\Lambda$  has or admits *Complex Multiplication*. It can be shown that if  $\Lambda$  has CM, then  $\omega$  belongs to a complex quadratic field  $K = \mathbb{Q}(\sqrt{\delta})$ . Then  $M(\Lambda)$  is an order of  $\mathcal{O}$  in  $K$ , that is a ring which is a free submodule of rank 2 over  $\mathbb{Z}$  of  $\mathcal{O}_K$ , the ring of integers of  $K$  [Shaf2] [Lang1] [Lang1].

### Class Field Theory of Imaginary Quadratic Fields:

Class Field Theory is one the most remarkable achievements of mathematics. One of its motivating problem was the construction of the maximal unramified Abelian extensions of an imaginary quadratic field. In the present context we need only small part of the theory.

Let  $-D = \delta$  be a fundamental dicriminant and  $K = \mathbb{Q}(\sqrt{\delta})$ . The *Hilbert Class Field* of  $K$  is the maximal unramified Abelian extension of  $K$  and is denoted by  $H_K$ . Now we have:

**Theorem 1:** The field  $H_K$  can be obtained by adjoining to  $K$  any value  $j_r = j(\omega_r)$ , where  $\omega_r$  is the complex number associated with  $Q_r$  i.e.  $\omega_r = \omega(Q_r) = (-b_r + \sqrt{\delta})/2a_r$  with  $Q_r = (a_r, b_r, c_r)$  in  $\mathcal{C}(\delta)$ . The minimal polynomial of the  $j_r$ 's is denoted by  $W_\delta[j](x)$ . It follows that  $H_K$  is precisely the splitting field of  $W_\delta[j](x)$ . The Galois group  $G_H$  of  $H_K/K = K(j(\omega_r))/K$  is isomorphic to  $\mathcal{C}(\delta)$ , the corresponding element  $\sigma_Q$  of  $G_H$  acts on  $j(Q')$  by

$$\sigma_Q(j(Q')) = j(Q^{-1} \cdot Q').$$

We also require the following:

**Theorem 2:** A rational prime  $p$  is a norm in  $K$  iff  $(p)$  splits completely in  $H_K$ . This is equivalent to saying that  $W_\delta[j](x) \pmod{p}$  has only simple roots and they are all in  $\mathbb{F}_p$ . Moreover, we have that

$$4p = A^2 + DB^2$$

has a solution in rational integers  $(A, B)$  iff  $W_\delta[j](x)$  splits completely modulo  $p$ . This last statement follows from the previous proposition about representation of  $4p$ .

Actually in the above,  $H_K$ , the Hilbert class field is the maximal unramified Abelian extension of  $K$  w.r.t the maximal order  $\mathcal{O}_K$ . As we have shown, we can associate an isomorphism between the form class group  $\mathcal{C}(\mathcal{O})$  of all quadratic forms of discriminant  $\delta$  and the ideal class group  $\mathcal{CL}(\mathcal{O})$ . That is to say, we can associate a *Ring Class Field*  $H_{\mathcal{O}}$  to an order  $\mathcal{O}$  in  $K$ . So the theorem 1 in the context of Class Field Theory stated above can be restated with what we spoke related to the class group  $\mathcal{CL}(\mathcal{O})$  of an order  $\mathcal{O}$  in  $K$ .

**Dedekind's  $\eta$ -Function and Weber's Functions  $f, f_1, f_2$ :** For  $\tau \in \mathbb{H}$  and  $a \in \mathbb{Q}$ , we put  $q = e^{2\pi i \tau a}$ . Let  $\zeta_n = e^{2\pi i/n}$ . The Dedekind  $\eta$ -function is defined by

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) = q^{1/24} \sum_{n=-\infty}^{\infty} (-1)^n q^{(3n^2+n)/2}.$$

Note that  $\eta(\tau)$  converges for  $\tau \in \mathbb{H}$ . The classical Weber functions  $f, f_1, f_2$  are defined in terms of  $\eta$  as follows:

$$f(\tau) = \zeta^{-1} \frac{\eta((\tau+1)/2)}{\eta(\tau)}$$

$$f_1 = \frac{\eta(\tau/2)}{\eta(\tau)}$$

$$f_2 = \sqrt{2} \frac{\eta(2\tau)}{\eta(\tau)}$$

The elliptic modular function  $j$ , is the cube root of  $\gamma_2$  and the functions  $\gamma_3$  and  $\gamma_2$  are connected to the Weber functions and  $j$  via

$$\begin{aligned}\gamma_2 &= \frac{f^{24} - 16}{f^8} = \frac{f_1^{24} + 16}{f_1^8} = \frac{f_2^{24} + 16}{f_2^8} \\ \gamma_3 &= \frac{(f^{24} + 8)(f_1^8 - f_2^8)}{f^8} \\ j &= \gamma_2^3 = \gamma_3^2 + 1728\end{aligned}$$

The action of the generators of  $SL_2(\mathbb{Z})$  on these functions is given by

$$\begin{aligned}\eta(\tau + 1) &= \zeta_{24} \eta(\tau) \\ f(\tau + 1) &= \zeta_{48}^{-1} f_1(\tau) \\ f_1(\tau + 1) &= \zeta_{48}^{-1} f(\tau) \\ f_2(\tau + 1) &= \zeta_{24} f_2(\tau) \\ \gamma_3(\tau + 1) &= -\gamma_3(\tau) \\ \gamma_2(\tau + 1) &= \zeta_3^{-1} \gamma_3(\tau) \\ j(\tau + 1) &= j(\tau) \\ \eta(-1/\tau) &= \sqrt{-i\tau} \eta(\tau) \\ f(-1/\tau) &= f(\tau) \\ f_1(-1/\tau) &= f_2(\tau) \\ f_2(-1/\tau) &= f_1(\tau) \\ \gamma_3(-1/\tau) &= -\gamma_3(\tau) \\ \gamma_2(-1/\tau) &= -\gamma_2(\tau) \\ j(-1/\tau) &= j(\tau)\end{aligned}$$

We also recall the useful relations

$$\begin{aligned}f \cdot f_1 \cdot f_2 &= \sqrt{2} \\ f_1(2\tau) &= f \cdot f_1(\tau)\end{aligned}$$

and

$$f^8 = f_1^8 + f_2^8$$

Now that we have seen the basic material which we will need, related to quadratic forms and quadratic fields and how elegantly Class Field Theory combines or links both of

these domains, let us recall certain basics regarding elliptic curves over a finite field, some of which we will adjust to our application.

**Theorem 1:** Let  $E$  be an elliptic curve over a finite field. Then the endomorphism ring (always considered over an algebraic closure)  $\text{End}(E)$  of  $E$  is either an order in an imaginary quadratic field  $K$  or an order in a quaternion algebra.

In the first case  $E$  is called *ordinary or non-supersingular* and in the second *supersingular*. Note that in any case,  $E$  has complex multiplication since  $\text{End}(E)$  is strictly larger than  $\mathbb{Z}$ . The following theorem enables us to distinguish between ordinary and supersingular curves. For a complete classification of supersingular curves see [Huse].

**Theorem 2:** (1). An elliptic curve over  $\mathbb{F}_p$ ,  $p > 3$ , is supersingular, iff its group has cardinality  $p + 1$ .

(2). An elliptic curve over  $\mathbb{F}_{2^n}$  is supersingular, iff its  $j$ -invariant is zero.

Of course, in order to construct a curve with given order  $m = \#E(\mathbb{F}_q)$ ,  $q = p^n$ , we make use of the fact that the Riemann hypothesis for the  $\zeta$ -function of  $E$  over  $\mathbb{F}_q$  is true.

**Theorem 3:** (*Hasse's Theorem*). The order  $m = \#E(\mathbb{F}_q)$  of an elliptic curve  $E$  over  $\mathbb{F}_q$  satisfies the inequality:

$$|q + 1 - m| \leq 2\sqrt{q}$$

*Elliptic curves  $E$  over  $\mathbb{F}_q$  can be obtained by reducing suitable elliptic curves over algebraic number fields.*

**Theorem 4:** Let  $K$  be an imaginary quadratic field and  $H_{\mathcal{O}}$  be the ring class field associated to an order  $\mathcal{O}$  in  $K$ . Denote by  $p$  a rational prime which completely splits in  $K$  and by  $\mathcal{B}$  a prime of  $H_{\mathcal{O}}$  above  $p$  with residue degree  $f = f_{\mathcal{B}|p}$  and such that  $[\mathcal{O}_K : \mathcal{O}] \notin \mathcal{B}$ . Let  $\mathcal{E}$  be an elliptic curve over  $H_{\mathcal{O}}$  which has complex multiplication by  $\mathcal{O}$  and good, ordinary reduction at  $\mathcal{B}$ . Then there is an element  $\pi \in \mathcal{O}/p\mathcal{O}$  satisfying the system of norm equations

$$q = N_K(\pi)$$

$$\#E(\mathbb{F}) = N_K(1 - \pi)$$

for the  $\mathcal{B}$ -reduced curve  $E$  of  $\mathcal{E}$ , where  $q = p^f$ . The endomorphism ring of  $\mathcal{E}$  is stable under the reduction map  $\mathcal{E} \rightarrow E$  by  $\mathcal{B}$  i.e.  $\text{End}(\mathcal{E}) = \text{End}(E) = \mathcal{O}$ . Moreover, every elliptic curve over  $\mathbb{F}_q$  with endomorphism ring  $\mathcal{O}$  arises in this way.

Let  $\pi_q \in \text{End}(E)$  be the *Frobenius endomorphism* acting on  $E(\mathbb{F}_q)$  acting under the projection  $\mathcal{E} \rightarrow E$  by  $\mathcal{B}$  and the endomorphism  $1 - \pi \in \text{End}(\mathcal{E})$  maps to  $1 - \pi_q \in \text{End}(E)$ ,

where 1 is the identity endomorphism of both  $\mathcal{E}$  and  $E$ . The crucial point with respect to the construction is that the group of rational points of  $E$  is given as the kernel of  $1 - \pi_q$ . Thus, we want to find an elliptic curve  $\mathcal{E}$  over  $H_{\mathcal{O}}$  such that the reduced curve  $E$  over  $\mathbb{F}_q$  has the preassigned order

$$m = \#E(\mathbb{F}_q) = \#ker(1 - \pi_q).$$

First of all, we must find the imaginary quadratic field  $K$  of Theorem 4 when  $m$  and  $q$  are given.

**Theorem 5:** The imaginary quadratic field  $K$  of Theorem 4 is given by

$$K = \mathbb{Q}(\sqrt{(q+1-m)^2 - 4q}).$$

Concerning the group structure, we have

**Theorem 6:** (Hasse). Let  $E$  be an elliptic curve over the finite field  $\mathbb{F}_q$ . Then the structure of  $E$  as an Abelian group is given by

$$E(\mathbb{F}_p) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

where  $n_1$  and  $n_2$  are positive integers such that  $n_1 \mid n_2$  and  $n_1 \mid \gcd(\#E(\mathbb{F}_p), p-1)$ .

As a matter of fact, elliptic curves over prime fields are almost always cyclic. The following Theorem 7, helps us in deciding whether or not for any given  $n > 1$ , there is an elliptic curve  $E$  over  $\mathbb{F}_p$  with structure  $E(\mathbb{F}_p) \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ .

**Theorem 7:** Let  $E$  be an elliptic curve over  $\mathbb{F}_p$  with  $n = n_1 = n_2$  as in the preceding theorem. Then one of the statements

1.  $\text{End}(E)$  is an order of  $\mathbb{Q}(\sqrt{-1})$  and  $p = n^2 + 1$ .
  2.  $\text{End}(E)$  is an order of  $\mathbb{Q}(\sqrt{-3})$  and  $p = n^2 \pm n + 1$ .
- is true.

Having looked into all the basic material required, let us now look into the actual computational procedure for the *construction of elliptic curves with given group order over large finite fields* [LayZ]. For which the *reduced class equations* which are useful in the effective construction of the Ring Class Fields associated to an order of a imaginary quadratic fields because it forms the main part of the procedure. (the terminology and the notations will be the same as above i.e have the same meaning)

### Reduced Class Equations:

Let  $u(z)$  denote a modular function and  $\omega = \omega(\mathcal{O}) = \tau_{Q_0}$  be the generator of  $\mathcal{O}$  such that  $\mathcal{O} = \mathbb{Z} + \omega\mathbb{Z} = \mathbb{Z} + [\mathcal{O}_K : \mathcal{O}]\omega_K\mathbb{Z}$ , where  $\omega_K = \omega(\mathcal{O}_K)$ . Then as we have seen Weber's extension of the concept of Class Invariants,  $u(z)$  is a Class Invariant, if  $u(z) \in H_{\mathcal{O}} = K(j(\omega))$ . We then write the minimal polynomial of  $u(z)$  over  $\mathbb{Q}$ . Note that  $W_{\delta}[j]$  is just the usual *Class*



Equation corresponding to the discriminant  $\delta$ . We define

$$\begin{aligned}\gamma_2^*(Q) &= \zeta_3^{(a-c+a^2c)} \gamma_2(\tau_Q) \\ \gamma_3^*(Q) &= (-1)^{(a+c+ac)(b-1)/2} \gamma_3(\tau_Q) \\ f^*(Q) &= \begin{cases} \zeta_{48}^{(a-c-ac^2)b} f(\tau_Q) & \text{if } 2 \mid a \text{ and } 2 \mid c \\ (-1)^{(\delta-1)/8} \zeta_{48}^{(a-c-ac^2)b} f_1(\tau_Q) & \text{if } 2 \mid a \text{ and } 2 \nmid c \\ (-1)^{(\delta-1)/8} \zeta_{48}^{(a-c+a^2c)b} f_2(\tau_Q) & \text{if } 2 \nmid a \text{ and } 2 \mid c \end{cases}\end{aligned}$$

In the following Table(Choice of  $u$ ) we will see some functions(relation between  $j$  and  $u$ )  $\psi_u(x)$  introduced by Lay & Zimmer [LayZ] which they have derived and used to compute  $W_\delta[j](x)$  efficiently. In particular, since  $u(\omega)$  is algebraic over  $\mathbb{Z}$  and not  $\mathbb{R}$  and that we are computing first  $W_\delta[u](x)$  using real number approximations (which is of course our strategy) which will give a polynomial over  $\mathbb{R}$ , and then using the relation  $\psi_u(x)$  between  $u$  and  $j$  to get  $W_\delta[j](x)$  there is a need to define a *required precision*. In particular, we use the following precision(decimal) function in our computations (For the derivation of which, see [AtMo]):  $\Pi_u$  and is defined as

$$\Pi_j = 5 + h/4 + \frac{\pi\sqrt{-\delta}}{\ln 10} \sum_{[a,b,c] \in C(\delta)} a^{-1}$$

TABLE(Choice of  $u$ )

$$\delta = 1 \Rightarrow u = j, u^* = j, \psi_u(x) = x \Pi_u = \Pi_j$$

$$\delta \not\equiv 0 \pmod{2} \Rightarrow u = \sqrt{\delta} \gamma_3, u^* = \sqrt{\delta} \gamma_3^*, \psi_u(x) = x^2/\delta + 1728, \Pi_u = (\Pi_j + h \log_{10} |\delta|)/2$$

$$\delta \not\equiv 0 \pmod{3} \Rightarrow u = \gamma_2, u^* = \gamma^*, \psi_u(x) = x^3, \Pi_u = \Pi_j/3$$

$$\delta \not\equiv 0 \pmod{3}, \delta \equiv 1 \pmod{8} \Rightarrow u = (-1)^{(\delta-1)/8} \zeta_{48} f_2, u^* = f^*, \psi_u(x) = (x^{24} - 16)^3/x^{24},$$

$$\Pi_u = 1 + \Pi_j/47$$

**Theorem 9:** Let  $\delta$  be the discriminant of an order  $\mathcal{O}$  in  $\mathbb{Q}(\sqrt{\delta})$  and choose  $\delta, u, u^*$  and  $\psi_u$  according to the Table 1. Then

1.  $u^*$  depends only on the  $SL_2(\mathbb{Z})$ -equivalence classes of  $Q$ , so that we may write  $u^*([Q])$  for  $u^*(Q)$ .

2.  $u^*([Q_0]) \in \mathbb{Q}(j([Q_0]))$  where  $[Q_0]$  is the class of the principal form  $Q_0$  hence is the identity in  $\mathcal{C}(\delta)$ .
3.  $u^*([Q]) = \tilde{u}^*([Q])$  where the tilde denotes complex conjugation and  $-[Q]$  stands for the inverse of  $[Q]$ , i.e.  $-[a, b, c] = [a, -b, c]$ .
4.  $W_\delta[u](x) = \prod_{[Q] \in \mathcal{C}(\delta)} (x - u^*([Q]))$
5.  $W_\delta[u](x_0) = 0 \Rightarrow W_\delta[j](\psi_u(x_0)) = 0$

We now summarize the steps required for computing  $W_\delta[u]$ :

1. Compute  $\mathcal{C}(\delta)$  by means of the Theorem which we saw in the context of the relation between ideal classes and forms, above.
2. Compute approximations  $\tilde{u}^*([Q])$  for the  $h(\mathcal{O})$  values  $u^*([Q])$ . Apply Theorem 9 to speedup the computation.
3. Form the product (Theorem 9.4) to obtain a polynomial  $\tilde{W}_\delta[u](x) \in \mathbb{R}[x]$  corresponding to  $\tilde{u}^*([Q])$ .
4.  $W_\delta[u]$  will be *close* to the desired Class equation  $W_\delta[u](x) \in \mathbb{Z}[x]$ , provided the operations have been carried out with a sufficiently high precision  $\Pi_u$ .
5. Round  $\tilde{W}_\delta[u]$  to obtain  $W_\delta[u]$ , i.e. round its coefficients.

Since  $u^*$  depends only on  $[Q] \in \mathcal{C}(\delta)$ , we may represent the elements of  $\mathcal{C}(\delta)$  by the unique reduced quadratic forms  $Q = (a, b, c)$  of discriminant  $\delta$ . Thus, we have  $|b| \leq a \leq \sqrt{-\delta/3}$ , and the Dedekind  $\eta$ -function converges at worst like a power series in  $e^{-\pi\sqrt{3}}$ .

Since we have looked into how to construct the Class equation, let us now see how to construct an elliptic curve having a group order  $m$  over  $\mathbb{F}_p$ . For which we need to have the *defining equation* of an elliptic curve in terms of its  $j$ -invariant. Let us again look into the reduction, stated in Theorem 4.

### A Defining Equation:

The finite field  $\mathbb{F}_q$  and the order of the elliptic curve  $E$  over  $\mathbb{F}_q$  are connected by the two norm equations. By Class Field Theory, we know that the class invariant  $u$  associated to the  $j$ -invariant of  $\mathcal{E}$  by  $\psi_u$  defined above, is a primitive element of the Ring Class Field  $H_{\mathcal{O}}$  over  $K$ , that is

$$H_{\mathcal{O}} = K(j(\mathcal{E})) = K[x]/W_{\delta(\mathcal{O})}[u](x)K[x].$$

Note that by the decomposition law for primes in an algebraic number field and by the algebraic properties of  $H_{\mathcal{O}}$  and  $\mathcal{B} \subset H_{\mathcal{O}}$  ( $p$  splits completely in  $K$  and is relatively prime to the conductor of  $\mathcal{O}$ ) it is easy to see that the reduced class equation  $W_{\delta}[u]$  splits over  $\mathbb{F}_p$  into irreducible factors of degree  $f = f_{\mathcal{B}|p}$  [Cohn1][Heck][Shaf2][Lang2][BCIS]. This is true because the  $\mathcal{B}$  in Theorem 4 has residue field  $\mathcal{O}_{H_{\mathcal{O}}}/\mathcal{B} \cong \mathbb{F}_q$ , where  $q = p^f$  [BCIS][Cohn1]. Observe also that, for each root  $x_0$  of  $W_{\delta}[u] \bmod \mathcal{B}$ ,  $\psi_u(x_0)$  yields the image of the  $j$ -invariant under the reduction modulo  $\mathcal{B}$  of an elliptic curve  $\mathcal{E}$  over  $H_{\mathcal{O}}$  with endomorphism ring  $\text{End}(\mathcal{E}) = \mathcal{O}$ , and hence yields the  $j$ -invariant of an elliptic curve  $E$  over  $\mathbb{F}_p$  with group order  $N_K(1 - \alpha\pi)$  for  $\alpha \in \mathcal{O}_K^*$ . Therefore, the computation of a defining equation consists in the following steps:

1. Compute/choose  $\delta$  and a prime  $p$  that splits completely in  $K = \mathbb{Q}(\sqrt{\delta})$ .
2. Choose the class invariant  $u$  of Table 1 that requires the lowest precision  $\Pi_u$ .
3. Compute  $W_{\delta}[u]$ .
4. Find a root  $x_0$  of  $W_{\delta}[u]$  over  $\mathbb{F}_q$ .
5. Put  $j_0 = \psi_u[x_0]$ .
6. Compute an elliptic curve over  $\mathbb{F}_q$  with  $j$ -invariant  $j_0$  having the desired group order  $m = \#E(\mathbb{F}_q) = \#ker(1 - \pi)$ .

It remains to explain the last step. We need a relation between the  $j$ -invariant and the curve. Instead of using the usual (long) Weierstrass equation for solving this problem, we prefer to employ other normal forms which are more appropriate with respect to our problem.

**Theorem 10:** (1). Let  $p > 3$  be a prime and  $j_0 \in \mathbb{F}_p$  be given. Then the elliptic curve over  $\mathbb{F}$

$$\begin{aligned} E : y^2 &= x^3 + 3kx + 2k & \text{with } k &= \frac{j_0}{1728 - j_0} \text{ if } j_0 \neq 0, 1728 \\ E : y^2 &= x^3 + ax & \text{with } a &\in \mathbb{F}_p^* \text{ if } j_0 = 1728 \\ E : y^2 &= x^3 + b & \text{with } b &\in \mathbb{F}_p^* \text{ if } j_0 = 0 \end{aligned}$$

has  $j$ -invariant  $j_0$ .

(2). Let  $\gamma \in \mathbb{F}_{2^n}$  be given with absolute trace  $\text{Tr}(\gamma) = 1$ . Then a complete set of isomorphism classes of ordinary (which is equivalent to  $j \neq 0$  in characteristic 2) elliptic curves over  $\mathbb{F}_{2^n}$  is given by

$$y^2 + xy = x^3 + a_2x^2 + j^{-1} \text{ with } a_2 \in \{0, \gamma\}.$$

But unfortunately, by the reduction process of Theorem 4, every isomorphism class of elliptic curves over  $H_{\mathcal{O}}$  splits into several isomorphism classes of elliptic curves over  $\mathbb{F}_q$ . That is, an isomorphism class of elliptic curves over  $\mathbb{F}_q$  is not uniquely determined by its  $j$ -invariant. The number of these isomorphism classes (for a fixed invariant) is given by the number  $\#\mathcal{O}_K^*$  of units in  $K$ . (This is clear because the solution of the norm equation is unique upto multiplication with an unit, since  $N_K(\pi) = N_K(\alpha\pi) = N_K(\alpha)N_K(\pi)$  because  $N_K(\alpha) = 1$  for  $\alpha \in \mathcal{O}_K^*$  [Poll][Cohn1]. We shall need the following:

**Theorem 11:** Let  $E$  and  $E'$  be two elliptic curves over  $\mathbb{F}_q$ . If  $E$  is ordinary then  $E$  and  $E'$  are isomorphic iff  $j(E) = j(E')$  and  $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ .

Let the elliptic curve  $E$  over  $\mathbb{F}_p, p > 3$ , be given by a short Weierstrass equation

$$E : y^2 = x^3 + ax + b.$$

Define the  $c$ -twist  $\tilde{E}$  of  $E$  by

$$\tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b} \text{ with } \tilde{a} = ac^2 \text{ and } \tilde{b} = bc^3$$

for any fixed non-square  $c \in \mathbb{F}_p^*$ . In characteristic 2, we define the  $\gamma$ -twist of

$$E : y^2 + xy = x^3 + a_2x^2 + a_6$$

by

$$\tilde{E} : y^2 + xy = x^3 + \tilde{a}_2x^2 + \tilde{a}_6 \text{ with } \tilde{a}_2 = a_2 + \gamma \text{ and } \text{Tr}(\gamma) = 1.$$

**Theorem 12:** Let  $E$  be an ordinary curve over  $\mathbb{F}_q$  and  $\tilde{E}$  be a twist. Then

1.  $j(E) = j(\tilde{E})$
2.  $\#E(\mathbb{F}_q) + \#\tilde{E}(\mathbb{F}_q) = 2q + 2$
3.  $E(\mathbb{F}_{q^2}) \cong \tilde{E}(\mathbb{F}_{q^2})$

In the case of  $\delta(K) < -4$ , there are only two isomorphism classes. The defining equation of a curve satisfying  $m = \#E(\mathbb{F}_q) = \#\ker(1 - \pi)$  is then given by  $E$  or its twist  $\tilde{E}$ , where  $j(E) = j(\tilde{E}) = j_0$ . In any case, the right choice between  $E$  and  $\tilde{E}$  is made by trial and error for  $p > 3$ . If  $p = 2$ , we have

**Theorem 13:** Let  $E$  be an ordinary elliptic curve over  $\mathbb{F}_{2^n}$  in the normal form. Then

$$\#E(\mathbb{F}_{2^n}) \equiv 2\text{Tr}(a_2) \pmod{4}$$

Now that we have seen the procedure to design or to say construct a curve of given group order over a large finite field, let us see if there are any computational problems with

the above procedure. The main problem sometimes would be that , for the given group order  $m = \#E(\mathbb{F}_p)$  and prime  $p$ , the chosen field  $K = \mathbb{Q}(\sqrt{(p+1-m)^2 - 4p})$  might have a very large discriminant (squarefree part of  $(p+1-m)^2 - 4p$ ) and/or a very large class number, which will reduce the speed of computation very severely. But at times when we *design* the (large) order  $m$  and the (large) prime  $p$ , we can mend our procedure so that we can work with a small class number. That is to say, if we are not bothered about a *specific* value of  $m$  and  $p$ , but we impose the condition that they be large (which can be stated for example by giving a bound like  $m = 2q'$ ,  $q' \geq 10^{50}$ ), we can start with a small class number  $h_K$  and proceed on to find an integral solution for the norm equation  $N_K(\pi) = m$  such that  $N_K(1 - \pi)$  or  $N_K(1 + \pi)$  is prime. This way, we are sure to work with a small class number and find the corresponding discriminant and hence design a suitable curve efficiently with less time of computation. Note that in cryptographic applications, this will be the case mostly where we will be asked for ordinary curves.

From the above discussion, it is clear that in the other method with relaxed constraints, solving the norm equation forms the major part. So in the next section let us see an effective way of solving the norm equation.

### 5.3 Solving the Norm Equation

We want to compute all representations of a positive integer  $m$  as a norm in the imaginary quadratic field  $K = \mathbb{Q}(\sqrt{\delta})$  of discriminant  $\delta = \delta_K$ . Equivalently, we must find the generators of all principal ideals of  $\mathcal{O}_K$  with norm  $m$  [Heck] [Shaf1] [Shaf2] [Ono] [PoZe]. We write

$$m = \prod_{p|m} p^{e_p}$$

and

$$p\mathcal{O}_K = \begin{cases} \mathcal{P}^2 & \text{with } \mathcal{N}(\mathcal{P}) = p \text{ if } (\delta | p) = 0 \\ \mathcal{P}\bar{\mathcal{P}} & \text{with } \mathcal{N}(\mathcal{P}) = p \text{ if } (\delta | p) = 1 \\ \mathcal{P} & \text{with } \mathcal{N}(\mathcal{P}) = p^2 \text{ if } (\delta | p) = -1 \end{cases}$$

where  $(\cdot | p)$  denotes the Legendre symbol  $\lambda_p(\cdot)$  for  $p \neq 2$  and the Kronecker symbol for  $p = 2$  i.e.

$$(\delta | 2) = \begin{cases} -1 & \text{if } \delta \equiv 5 \pmod{8} \\ 0 & \text{if } \delta \equiv 0 \pmod{4} \\ 1 & \text{if } \delta \equiv 1 \pmod{8} \end{cases}$$

If  $e_p$  is odd for one  $p$  with  $(\delta | p) = -1$ , then there is no ideal of norm  $m$  in  $\mathcal{O}_K$ . Otherwise, the ideals  $\mathcal{A}$  of norm  $m$  are obviously given by

$$\mathcal{A} = \prod_{\mathcal{P}|m, (\delta|p)=0} \mathcal{P}^{e_p} \prod_{\mathcal{P}|m, (\delta|p)=1} \mathcal{P}^{e_p - k_p} \bar{\mathcal{P}}^{k_p} \prod_{\mathcal{P}|m, (\delta|p)=-1} \mathcal{P}^{e_p/2}, \text{ with } 0 \leq k_p \leq e_p.$$

In order to decide or not an ideal  $\mathcal{A}$  is principal, we consider  $\mathcal{A}$  as a lattice in  $\mathbb{C}$  and look for a minimal (with respect to the norm  $N_K$ ) element  $\pi$  of  $\mathcal{A} - \{0\}$ . Since  $\mathcal{A}$  is principal iff  $N_K(\pi) = \mathcal{N}(\mathcal{A}) = m$  and  $\pi$  is unique upto the known units of  $K$ , we find all solutions to  $m = N_K(\pi)$  with  $\pi \in \mathcal{O}_K$ . To get an explicit representation of a prime ideal  $\bar{\mathcal{P}}$ , we use the decomposition law. The prime ideal  $\mathcal{P}$  is given (up to conjugation) by

$$\mathcal{P} = \begin{cases} p\mathcal{O}_K & \text{if } (\delta | p) = -1 \\ p\mathcal{O}_K + (\omega_K - \omega_p)\mathcal{O}_K & \text{if } (\delta | p) \in \{0, 1\}, \end{cases}$$

where  $\omega_p \in \mathbb{Z}$  is any solution of  $\omega_p \equiv \omega_K \pmod{p}$ . Note that  $\mathcal{O}_K = \mathbb{Z} + \omega_K \mathbb{Z}$ . From this it is easy to derive a  $\mathbb{Z}$ -basis for  $\mathcal{P}$ . In particular, we have

$$\begin{aligned} \mathcal{P} &= p\mathbb{Z} + \frac{r + \sqrt{\delta}}{2} \text{ with} \\ r^2 &\equiv \delta \pmod{4p} \text{ if } p \neq 2, (\delta | p) = 1 \\ r &= p\delta \text{ } p \neq 2, (\delta | p) = 0 \\ r &= \delta \text{ } p = 2, (\delta | p) = 1 \\ r &= \delta/2 \text{ } p = 2, (\delta | p) = 0 \end{aligned}$$

Having seen how to solve the norm equation, let us look into how, elliptic curves over  $\mathbb{F}_{2^n}$  useful for cryptographic purposes can be constructed. Based on discrete logarithms and MOV attack, the elliptic curves (non-supersingular) which are suitable are those with the group order  $m = \#E(\mathbb{F}_{2^n}) = c \cdot q$  with  $q$  a prime and  $c \leq c_{max}$ . The constant  $c_{max}$  decides, in which larger extension (of  $\mathbb{F}_{2^n}$ ), one has to work the discrete log problem (DLP) in order to crack Elliptic DLP, based on MOV attack [Men1].

We choose  $n$  based on other features like existence of a ONB or a convenient irreducible polynomial e.t.c. We look for an imaginary quadratic field  $K$  of class number  $n$  such that 2 splits completely in  $K$ , i.e.  $\delta_K \equiv 1 \pmod{8}$ , and solve  $2^n = N_K(\pi)$  for  $\pi \in \mathcal{O}_K/2\mathcal{O}_K$ . For  $m = N_K(1 - \pi)$  of the form  $m = c \cdot q_*$  with  $q_*$  a prime ( $*$  will indicate the number of decimal digits of  $q_*$ ) and  $c \leq c_{max} = 100$  or so, we succeed. If we took  $K$  to have a divisor of  $n$  as class number, then  $m$  would not be of the desired form  $m = c \cdot q_*$  because we then would have a representation  $m = N_K(1 - \pi^{n/h(K)})$  and  $m$  could not have a large prime divisor  $q_*$ . We only look for  $K$ 's with  $\delta_K \not\equiv 0 \pmod{3}$  which enables us to use the Yui-Zagier reduced Class equation  $W = W_\delta[f^*]$ . The polynomial  $W$  is clearly irreducible over  $\text{GF}(2)$  and we can use it to generate  $\mathbb{F}_{2^n}$ . A root of  $W \pmod{2}$  over  $\mathbb{F}_{2^n}$  is then trivially computed and from the last row of the Table 1, we get  $j(E) = \varrho^{48}$ . That is

$$\mathbb{F}_{2^n} \cong \mathbb{F}_2/W\mathbb{F}_2[x] \cong \mathbb{F}_2(\varrho), \text{ where } W(\varrho) = 0$$

$$\alpha = \sum_{i=0}^{n-1} \alpha_i \varrho^i \in \mathbb{F}_2(\varrho), \alpha_i \in \mathbb{F}_2$$

## Chapter 6

# Results and Conclusion

In this chapter, we will see the results of implementation of all computational procedures which we saw in the previous chapters along with the underlying theory. We will first list the results related to finite field arithmetic and later look into the actual the design of elliptic curves suitable for public-key cryptosystems. We also include the results related to the implementation of Elliptic Curve Cryptosystems.

### 6.1 Normal Basis Arithmetic

To get the bilinear form  $c_0 = \bar{A}\Lambda\bar{B}^T$  required for implementing the arithmetic operation of multiplication w.r t the chosen ONB, a general program has been written. The program is based on what we have derived in the Chapters 3 & 4. This program will give  $c_0$  in the expanded form, and hence, is suitable for direct implementation. That is, it gives  $c_0$  in the form

$$c_0 = a_0b_1 + a_1(b_{(1)} + b_{(2)}) + \dots$$

The correctness of the derived formula has been checked by verifying

$$C = A \cdot B = B \cdot A \text{ and } A \cdot 1 = 1 \cdot A \text{ and } A \cdot A^{-1} = 1$$

A program which will enable us to get the matrix of transformation from any basis to any other basis has also been written, the theory for which, we saw in the Chapter 4.

A search for other irreducible polynomials using randomoized algorithms [Men2], in the fields having ONB has also been done. The results of the search for the extensions  $\text{GF}(2^{239})$ ,  $\text{GF}(2^{281})$  and  $\text{GF}(2^{333})$  are that we have the following irreducible polynomials:

$$x^{239} + x^{36} + 1$$

$$x^{281} + x^{93} + 1$$

$$x^{333} + x^{99} + 1$$

These can be used to generate a polynomial basis.

## 6.2 Elliptic Curve Cryptosystems

For the implementation of elliptic curve cryptosystems, the number-theoretic package, SIMATH ver 3.9 has been used. For certain other off-line computations the package PARI/GP has also been used. For all the underlying computations, the currently best known (computational) algorithms have been studied and used. We have written a fairly general program in that, the choice of the curve can be made at run-time from a file. Now let us see the implementation details of ElGamal scheme for public key encryption.

*ElGamal scheme:* This is another public key cryptosystems for transmitting messages  $m \Rightarrow P_m$ . As in the key exchange system[Kob1], we start with a fixed publicly known finite field  $\mathbb{F}_q$ , elliptic curve  $E$  defined over it, and base point  $P \in E$ . (We do not need to know the number of points  $\#E(\mathbb{F}_q)$ .) Each user chooses a random integer  $n$ , which is kept secret, and publishes the point  $n \cdot P$ .

To send a message  $P_m$  to user  $B$ , user  $A$  chooses a random integer  $k$  and sends the pair of points  $(k \cdot P, P_m + k(k_B \cdot P))$  (where  $k_B \cdot P$  is user  $B$ 's public key). To read the message, user  $B$  multiplies the first point in the pair by his secret  $k_B$  and subtracts the result from the second point:

$$P_m + k(k_B \cdot P) - k_B(k \cdot P) = P_m$$

Thus user  $A$  sends a disguised  $P_m$  along with a *clue*  $k \cdot P$  which is enough to remove the *mask*  $k(k_B \cdot P)$  if one knows the secret integer  $k_B$ . An evesdropper who can solve the discrete log problem on  $E$  (EDLP) can, of course, determine  $k_B$  from the publicly known information  $P$  and  $k_B \cdot P$ .

So the main steps involved are as follows:

1. Selecting a random point 'P',  $k_A, k_B$ , and  $k$ .
2. Mapping the message (see chapter 4 for details of the algorithms used) to a point on the curve. i.e.  $m \rightarrow P_m$
3. Computing  $k \cdot P$  and  $P_m + k \cdot (k_B \cdot P)$ .

We used the ASCII characters as numbers from 000 to 255. Each message was chosen to be of 10 ASCII characters, and hence we have to work with a curve defined over a field  $\text{GF}(p)$  where  $p$  is a prime having more than 30 digits (since 10 ASCII characters, each a three digit number between 000 and 255, would give a maximum number  $255255 \dots 255$  having  $3 \times 10$  digits) An experimentally observed fact regarding message mapping rule which was suggested by N.Koblitz [Kob1] was that it was very efficient in that, over a large finite field, on an average it required only 3 to 4 trials to be successful. The main time consuming steps are the Legendre symbol computation, solution of the quadratic, and of course computing  $k$  times a point. For the computation of  $k$  times of a point, we can



use the addition-subtraction chains method suggested by Staffelbach. For core arithmetic operations, it is found that the arithmetic package PARI and/or MIRACLE is/are well suited.

### 6.3 Design of Elliptic Curves

All the computational aspects and theory related to the design of curves have been discussed in Chapter 4. For design also, we used the package SIMATH. After looking into the implementation details of some of the routines which are useful in the design of elliptic curves, it is suggested that for all the off-line computations (in fact the design of curves is invariably off-line) we can use SIMATH. The various curves over  $\mathbb{F}_p$  as well as  $\mathbb{F}_{2^n}$  which were designed using SIMATH are listed below as examples:

### Curves Over $\text{GF}(p)$ :

Here we give the  $p$  value, the discriminant  $\delta_K$  selected, and the corresponding class number  $h_K$ . The curves are specified by the Weierstrass short normal form  $y^2 = x^3 + ax + b \Rightarrow EC(a, b)$  and their orders by  $m = \#E(\mathbb{F}_p)$ .

```
in : p1 = 1040 + 121, : p1 = 100000000000000000000000000000000000000121.
```

$$\text{discriminant} = -67$$

class number = 1

```
out  m =100000000000000000000187300599782321059201:  EC(65610556376660448245
43989193463688093337, 4374037091777363216362659462309125395558)
```

out:  $m = 99999999999999999812699400217678941043$ :  $EC(68685909243073279646$   
 $86734696635115775535, 2924361375024414926768705033371681165977)$

-187

class number = 2

```
out: m =10000000000000000000176014087816420396971: EC(22705551197360737921
63330776700277340914, 6826570567784733511010165536483478846906)
```

out:  $m = 99999999999999999823985912183579603273$ :  $EC(88232059745032797029$   
 $48540359853664867516, 5882137316335519801965693573235776578344)$

-245

$$\text{class number} = 2$$

out:  $m = 100000000000000000067936536813851950100$ :  $EC(82648512469716035518$   
 $9218106558154784865, 7217656749798106903459478737705436523324)$







Here we are specifying the polynomials as a sequence of (exponent, coefficient) corresponding to the monomials having nonzero coefficients (This is also called "Sparse representation of polynomials"). For each example, we also explicitly give the values of  $[\delta_K, h_K, \Pi_{f^*}]$  (the decimal precision required), the selected  $c_{max}, q_*, c = \#E(\mathbb{F}_{2^n})/q_*$ , the number of imaginary quadratic fields  $K'$  having class number  $= h_K = n$  and  $\delta_{K'} \geq \delta_K$  which we denote as  $\nu_n(\delta_K), \nu_n(-1.6 \cdot 10^6)$ , in that order. We have used a dictionary that gives us a  $\delta_K$  for given  $h_K$  to reduce the time of search for the suitable imaginary quadratic field  $K$ .

For the field  $\text{GF}(2^{191})$ :

$$\delta_K = -87887, h_K = 191, \Pi_{f^*} = 81, c_{max} = 100, q_* = q_{58}, c = \#E(\mathbb{F}_{2^n})/q_* = 2^3 \cdot 3, \nu_n(\delta_K) = 10, \nu(-1.6 \cdot 10^6) = 184$$

The Reduced Class equation  $W_\delta[f^*] \bmod 2$ :

( 191 1 190 1 186 1 185 1 184 1 181 1 180 1 178 1 176 1 175 1 173 1 172 1 170 1 168 1 164 1 161 1 160 1 159 1 156 1 155 1 154 1 153 1 151 1 149 1 146 1 144 1 143 1 142 1 139 1 136 1 134 1 133 1 132 1 130 1 127 1 125 1 124 1 121 1 120 1 11 9 1 116 1 115 1 110 1 108 1 105 1 103 1 99 1 98 1 95 1 90 1 86 1 81 1 79 1 77 1 76 1 75 1 74 1 72 1 70 1 69 1 67 1 66 1 65 1 64 1 62 1 61 1 57 1 56 1 54 1 53 1 51 1 49 1 4 8 1 45 1 43 1 42 1 41 1 39 1 38 1 36 1 35 1 31 1 30 1 29 1 28 1 27 1 26 1 24 1 23 1 21 1 19 1 17 1 15 1 12 1 8 1 6 1 0 1 )

For the field  $\text{GF}(2^{293})$ :

$$\delta_K = -67559, h_K = 293, \Pi_{f^*} = 99, c_{max} = 100, q_* = q_{87}, c = \#E(\mathbb{F}_{2^n})/q_* = 2 \cdot 3 \cdot 5, \nu_n(\delta_K) = 2, \nu(-1.6 \cdot 10^6) = 127$$

The Reduced Class equation  $W_\delta[f^*] \bmod 2$ :

( 293 1 289 1 286 1 284 1 283 1 280 1 278 1 277 1 276 1 275 1 268 1 266 1 263 1 262 1 260 1 257 1 255 1 253 1 251 1 250 1 246 1 244 1 242 1 241 1 239 1 237 1 234 1 233 1 232 1 231 1 230 1 229 1 227 1 224 1 223 1 222 1 221 1 219 1 218 1 217 1 214 1 212 1 211 1 210 1 209 1 208 1 206 1 205 1 202 1 200 1 197 1 195 1 193 1 192 1 190 1 189 1 188 1 187 1 186 1 185 1 183 1 180 1 178 1 177 1 175 1 173 1 172 1 17 1 1 169 1 168 1 166 1 161 1 160 1 159 1 158 1 156 1 154 1 1 53 1 152 1 151 1 150 1 147 1 146 1 145 1 144 1 142 1 139 1 138 1 137 1 135 1 134 1 130 1 129 1 128 1 127 1 126 1 123 1 117 1 116 1 115 1 114 1 113 1 105 1 103 1 101 1 100 1 99 1 95 1 94 1 93 1 92 1 90 1 89 1 88 1 86 1 85 1 83 1 81 1 8 0 1 78 1 77 1 76 1 75 1 74 1 73 1 72 1 71 1 67 1 66 1 62 1 61 1 57 1 56 1 52 1 49 1 44 1 43 1 41 1 40 1 38 1 37 1 36 1 35 1 34 1 33 1 32 1 31 1 30 1 29 1 27 1 26 1 25 1 24 1 21 1 20 1 10 1 9 1 8 1 3 1 2 1 0 1 )

For the field  $\text{GF}(2^{300})$ :

$$\delta_K = -116087, h_K = 300, \Pi_{f^*} = 108, c_{max} = 100, q_* = q_{90}, c = \#E(\mathbb{F}_{2^n})/q_* = 2^2, \nu_n(\delta_K) = 22, \nu(-1.6 \cdot 10^6) = 2216$$

The Reduced Class equation  $W_\delta[f^*] \bmod 2$ :

$$\begin{aligned} & ( 300 \ 1 \ 298 \ 1 \ 297 \ 1 \ 293 \ 1 \ 292 \ 1 \ 291 \ 1 \ 289 \ 1 \ 286 \ 1 \ 284 \ 1 \ 283 \ 1 \ 281 \ 1 \ 279 \ 1 \ 27 \ 7 \ 1 \ 276 \ 1 \ 273 \ 1 \\ & 268 \ 1 \ 263 \ 1 \ 262 \ 1 \ 261 \ 1 \ 259 \ 1 \ 258 \ 1 \ 257 \ 1 \ 2 \ 56 \ 1 \ 253 \ 1 \ 252 \ 1 \ 248 \ 1 \ 246 \ 1 \ 245 \ 1 \ 244 \ 1 \ 243 \ 1 \\ & 239 \ 1 \ 237 \ 1 \ 236 \ 1 \ 234 \ 1 \ 231 \ 1 \ 230 \ 1 \ 227 \ 1 \ 226 \ 1 \ 225 \ 1 \ 223 \ 1 \ 222 \ 1 \ 218 \ 1 \ 217 \ 1 \ 213 \ 1 \ 212 \ 1 \ 208 \\ & 1 \ 207 \ 1 \ 206 \ 1 \ 204 \ 1 \ 201 \ 1 \ 199 \ 1 \ 197 \ 1 \ 195 \ 1 \ 190 \ 1 \ 189 \ 1 \ 187 \ 1 \ 186 \ 1 \ 182 \ 1 \ 179 \ 1 \ 178 \ 1 \ 177 \ 1 \\ & 172 \ 1 \ 171 \ 1 \ 170 \ 1 \ 168 \ 1 \ 166 \ 1 \ 165 \ 1 \ 161 \ 1 \ 160 \ 1 \ 159 \ 1 \ 157 \ 1 \ 156 \ 1 \ 155 \ 1 \ 153 \ 1 \ 152 \ 1 \ 148 \ 1 \ 146 \\ & 1 \ 145 \ 1 \ 144 \ 1 \ 141 \ 1 \ 140 \ 1 \ 137 \ 1 \ 136 \ 1 \ 135 \ 1 \ 134 \ 1 \ 133 \ 1 \ 130 \ 1 \ 128 \ 1 \ 124 \ 1 \ 123 \ 1 \ 122 \ 1 \ 12 \ 0 \ 1 \\ & 113 \ 1 \ 111 \ 1 \ 108 \ 1 \ 107 \ 1 \ 105 \ 1 \ 104 \ 1 \ 98 \ 1 \ 97 \ 1 \ 91 \ 1 \ 89 \ 1 \ 86 \ 1 \ 85 \ 1 \ 82 \ 1 \ 80 \ 1 \ 79 \ 1 \ 75 \ 1 \ 74 \ 1 \ 73 \\ & 1 \ 71 \ 1 \ 69 \ 1 \ 67 \ 1 \ 66 \ 1 \ 64 \ 1 \ 63 \ 1 \ 60 \ 1 \ 59 \ 1 \ 57 \ 1 \ 51 \ 1 \ 50 \ 1 \ 49 \ 1 \ 48 \ 1 \ 47 \ 1 \ 4 \ 6 \ 1 \ 42 \ 1 \ 41 \ 1 \ 38 \ 1 \ 37 \\ & 1 \ 36 \ 1 \ 32 \ 1 \ 31 \ 1 \ 30 \ 1 \ 27 \ 1 \ 26 \ 1 \ 24 \ 1 \ 22 \ 1 \ 21 \ 1 \ 20 \ 1 \ 16 \ 1 \ 13 \ 1 \ 12 \ 1 \ 11 \ 1 \ 8 \ 1 \ 7 \ 1 \ 6 \ 1 \ 4 \ 1 \ 3 \ 1 \ 0 \ 1 ) \end{aligned}$$

For the field  $\text{GF}(2^{307})$ :

$$\delta_K = -316759, h_K = 307, \Pi_{f^*} = 126, c_{max} = 100, q_* = q_{83}, c = \#E(\mathbb{F}_{2^n})/q_* = 2, \nu_n(\delta_K) = 24, \nu(-1.6 \cdot 10^6) = 145$$

The Reduced Class equation  $W_\delta[f^*] \bmod 2$ :

$$\begin{aligned} & ( 307 \ 1 \ 306 \ 1 \ 305 \ 1 \ 304 \ 1 \ 303 \ 1 \ 301 \ 1 \ 300 \ 1 \ 299 \ 1 \ 297 \ 1 \ 296 \ 1 \ 294 \ 1 \ 291 \ 1 \ 290 \ 1 \ 288 \ 1 \\ & 287 \ 1 \ 285 \ 1 \ 283 \ 1 \ 282 \ 1 \ 28 \ 1 \ 1 \ 277 \ 1 \ 276 \ 1 \ 275 \ 1 \ 274 \ 1 \ 272 \ 1 \ 269 \ 1 \ 267 \ 1 \ 265 \ 1 \ 264 \ 1 \ 2 \\ & 63 \ 1 \ 259 \ 1 \ 258 \ 1 \ 256 \ 1 \ 255 \ 1 \ 251 \ 1 \ 247 \ 1 \ 245 \ 1 \ 244 \ 1 \ 243 \ 1 \ 237 \ 1 \ 236 \ 1 \ 233 \ 1 \ 230 \ 1 \ 228 \\ & 1 \ 225 \ 1 \ 223 \ 1 \ 221 \ 1 \ 220 \ 1 \ 219 \ 1 \ 218 \ 1 \ 216 \ 1 \ 215 \ 1 \ 213 \ 1 \ 212 \ 1 \ 210 \ 1 \ 208 \ 1 \ 206 \ 1 \ 204 \ 1 \\ & 202 \ 1 \ 201 \ 1 \ 200 \ 1 \ 195 \ 1 \ 194 \ 1 \ 193 \ 1 \ 192 \ 1 \ 191 \ 1 \ 189 \ 1 \ 187 \ 1 \ 185 \ 1 \ 184 \ 1 \ 183 \ 1 \ 182 \ 1 \ 181 \\ & 1 \ 179 \ 1 \ 175 \ 1 \ 174 \ 1 \ 170 \ 1 \ 169 \ 1 \ 167 \ 1 \ 164 \ 1 \ 163 \ 1 \ 161 \ 1 \ 160 \ 1 \ 152 \ 1 \ 150 \ 1 \ 148 \ 1 \ 146 \ 1 \\ & 145 \ 1 \ 142 \ 1 \ 140 \ 1 \ 138 \ 1 \ 136 \ 1 \ 134 \ 1 \ 133 \ 1 \ 130 \ 1 \ 129 \ 1 \ 126 \ 1 \ 125 \ 1 \ 12 \ 4 \ 1 \ 122 \ 1 \ 121 \ 1 \\ & 120 \ 1 \ 118 \ 1 \ 115 \ 1 \ 114 \ 1 \ 113 \ 1 \ 112 \ 1 \ 108 \ 1 \ 1 \ 05 \ 1 \ 104 \ 1 \ 103 \ 1 \ 100 \ 1 \ 99 \ 1 \ 98 \ 1 \ 93 \ 1 \ 92 \ 1 \\ & 89 \ 1 \ 88 \ 1 \ 87 \ 1 \ 86 \ 1 \ 85 \ 1 \ 84 \ 1 \ 83 \ 1 \ 82 \ 1 \ 81 \ 1 \ 80 \ 1 \ 79 \ 1 \ 78 \ 1 \ 77 \ 1 \ 75 \ 1 \ 7 \ 4 \ 1 \ 73 \ 1 \ 72 \ 1 \ 71 \\ & 1 \ 70 \ 1 \ 68 \ 1 \ 67 \ 1 \ 62 \ 1 \ 57 \ 1 \ 52 \ 1 \ 50 \ 1 \ 49 \ 1 \ 48 \ 1 \ 47 \ 1 \ 46 \ 1 \ 44 \ 1 \ 41 \ 1 \ 40 \ 1 \ 39 \ 1 \ 37 \ 1 \ 36 \ 1 \\ & 35 \ 1 \ 34 \ 1 \ 33 \ 1 \ 26 \ 1 \ 24 \ 1 \ 23 \ 1 \ 21 \ 1 \ 18 \ 1 \ 17 \ 1 \ 15 \ 1 \ 14 \ 1 \ 13 \ 1 \ 11 \ 1 \ 9 \ 1 \ 8 \ 1 \ 5 \ 1 \ 4 \ 1 \ 3 \ 1 \ 2 \ 1 \ 1 \ 0 \ 1 ) \end{aligned}$$

For the field  $\text{GF}(2^{311})$ :

$$\delta_K = -281959, h_K = 311, \Pi_{f^*} = 135, c_{max} = 100, q_* = q_{92}, c = \#E(\mathbb{F}_{2^n})/q_* = 2 \cdot 5^2, \nu_n(\delta_K) = 23, \nu(-1.6 \cdot 10^6) = 128$$

The Reduced Class equation  $W_\delta[f^*] \bmod 2$ :

$$\begin{aligned} & ( 311 \ 1 \ 308 \ 1 \ 302 \ 1 \ 301 \ 1 \ 300 \ 1 \ 298 \ 1 \ 295 \ 1 \ 294 \ 1 \ 292 \ 1 \ 290 \ 1 \ 289 \ 1 \ 287 \ 1 \ 285 \ 1 \ 284 \ 1 \ 276 \ 1 \\ & 274 \ 1 \ 272 \ 1 \ 271 \ 1 \ 268 \ 1 \ 264 \ 1 \ 262 \ 1 \ 260 \ 1 \ 258 \ 1 \ 257 \ 1 \ 256 \ 1 \ 255 \ 1 \ 254 \ 1 \ 249 \ 1 \ 247 \ 1 \ 242 \ 1 \ 241 \end{aligned}$$

1 239 1 235 1 23 3 1 231 1 228 1 223 1 221 1 220 1 218 1 217 1 214 1 209 1 2 07 1 205 1 203  
1 201 1 200 1 199 1 198 1 197 1 196 1 195 1 194 1 190 1 188 1 187 1 186 1 184 1 182 1 181 1  
180 1 179 1 178 1 177 1 176 1 174 1 172 1 171 1 169 1 168 1 167 1 166 1 165 1 159 1 152 1 151  
1 148 1 146 1 145 1 143 1 142 1 137 1 135 1 133 1 132 1 131 1 129 1 127 1 125 1 124 1 123 1  
119 1 118 1 117 1 116 1 113 1 111 1 109 1 107 1 106 1 105 1 104 1 102 1 99 1 96 1 95 1 93 1  
91 1 90 1 87 1 85 1 79 1 77 1 76 1 75 1 74 1 71 1 70 1 69 1 66 1 63 1 61 1 56 1 53 1 49 1 48 1  
47 1 43 1 41 1 40 1 35 1 30 1 28 1 27 1 26 1 25 1 24 1 22 1 18 1 15 1 14 1 11 1 9 1 6 1 1 1 0 1 )

The main routines of SIMATH which were used in the design are as follows

sdiscclq:single discriminant, class equation: For building the class equation  $W_\delta[u](x)$

upmirfspec:univariate polynomial over modular integers root finding: To solve  $W_\delta[u](x)$

iecgnpj:integer elliptic curve of given number of points j-invariant: For getting the  $j$ -invariant of the curve having the given order.

iecjtoeqsv/iecjtoeq:integer elliptic curve with j-invariant given to equation: For getting the defining equation of the curve for which the j-invariant has been computed.

ecmpssa: elliptic curves over modular primes combined Schoof-Shanks algorithm: To find the order of an elliptic curve[Men1].

iprniqf: integer prime as a norm in quadratic field: To solve the norm equation of a prime.

iprpdqbqf: integer primary positive definite binary quadratic forms.

For solving the norm equation corresponding to a composite number, as we saw in the case of design of curves over  $\mathbb{F}_{2^n}$ , we first factorize the number and then use iprniqf (integer prime power as a norm in quadratic field).

## 6.4 Conclusions

After going through all the aspects involved in the design and implementation of Elliptic Curve Cryptosystems and after actual implementation using arithmetic packages SIMATH,PARI/GP, we have the following conclusions.

For implementing cryptosystems over  $\mathbb{F}_{2^n}$ , normal basis( specifically ONB) representa-

tion is the most suitable one in that, we can do almost all the computations quite efficiently. If we can allocate extra memory, we can achieve additional saving in time taken for certain computations.

For implementing arithmetic in  $\mathbb{F}_{2^m}$ , our specific routines are more efficient compared to those existing in the packages SIMATH and PARI/GP. For implementing the bilinear form for multiplication in terms of ONB, assembly level routines are to be written to have the maximum mults/sec. Since the design procedures have no restriction on the particular chosen field, we can always select a field which has an ONB (in fact even a PONB, if desired).

Coming to the case of cryptosystems over  $\mathbb{F}_p$ , the routines in SIMATH are suitable and are quite efficient for the design of suitable curves. But for implementing the cryptosystems, the routines of PARI and/or SIMATH can be used. The most time consuming part is the computation of Legendre character(symbol) encountered in message imbedding and solution of the quadratic congruence

$$y^2 = x_m^3 + ax_m + b \quad \lambda_p(x_m) = (x_m | p) = 1$$

where  $x_m$  is the number  $mk + j$  whose  $\lambda_p(x_m) = 1$  (refer Chapter 4 for message imbedding). We have very efficient ways of computing  $n \cdot P$  i.e.  $n$  times of a point  $P$ . But when compared with cryptosystems over  $\mathbb{F}_{2^m}$ , those over  $\mathbb{F}_p$  can be designed to be more secure, but the encryption time is more. Cryptosystems over  $\mathbb{F}_{2^m}$  can also be easily implemented in hardware because, representation of elements in terms of normal basis reduces addition of two elements into modulo 2 addition of the corresponding vectors (XORing) and multiplication can be performed in  $m$  clock cycles if the bilinear form of multiplication  $c_0$  is fused in hardware which for ONBs demands minimum number of cell interconnections.

For the implementation of a full fledged (that is, one that can be used for real time encryption) Elliptic Curve Cryptosystem, all the basic blocks are to be highly optimized e.g. the basic field arithmetic routines are to be written in assembly language. Our implementation was optimized only at the algorithm level.



# Bibliography

- [Abh] Abhyankar, S.S., *Algebraic Geometry for Scientists and Engineers*. AMS publications. 1984.
- [Alhf] Alhfors, L., *Complex Analysis: An Introduction to the Theory of Analytic Functions of One Complex Variable*. Mc Graw Hill, 1979.
- [AtMo] Atkin. O.A., Morain, F., "Elliptic Curves and Primality Proving", Math. of Comp. Vol-61, No-203, July 1993 29-68.
- [BCIS] Borel, A., Herz, C.S., Chowla, S., Iwasawa, K., Serre, J.P., *Seminar on Complex Multiplication*, Lecture Notes In Math, Vol-21. Springer Verlag, 1966.
- [Chah] Chahal. J.S., *Topics in Number Theory*. Plenum Press. 1986.
- [Cohn1] Cohn. H., *A Classical Invitation to Algebraic Numbers and Classfields*. Springer Verlag Universitext 1978.
- [Cohn2] Cohn. H., *A Second Course in Number Theory*. John Wiley & sons, 1981.
- [Casse] Cassels, J.W., *An Introduction to the Geometry of Numbers*. Springer Verlag series of comprehensive studies in mathematics. 1987.
- [Fult] Fulton, W., *Algebraic Curves*. Benjamin & Co. 1969.
- [GaV] Gao, S., Vanstone, "On Orders of Optimal Normal Basis Generators", Math. of Comp. Vol-64, No:211, July 1995, pp. 1227-1233.
- [Heck] Hecke, E., *Lectures in the Theory of Algebraic Numbers* Springer Verlag GTM No-77, 1981.
- [Huse] Husemoller, *Elliptic Curves*. Springer Verlag GTM No-111 1986.
- [Hasse] Hasse, H., *Number Theory* (3rd ed). Springer Verlag series of comprehensive studies in mathematics. 1979.

- [IrRo] Ireland, K., Rosen, M., *A Classical introduction to Modern Number Theory*. Springer Verlag GTM No-84, 1982.
- [Jones] Jones, B., *The Arithmetic of Quadratic Forms*. Carus Monograph No-10, 1961.
- [Kob1] Koblitz, N., *A Course in Number Theory and Cryptography*. Springer Verlag GTM No-114, 1989.
- [Kob2] Koblitz, N., *Introduction to Elliptic Curves and Modular Forms*. Springer Verlag GTM No-97, 1984.
- [Kara] Karatsuba, A., *Complex Analysis in Number Theory*. CRC press, 1995.
- [Lang1] Lang, S., *Algebra* (2nd ed). Addison Welsey, 1984.
- [Lang2] Lang, S., *Algebraic Number Theory*. Springer Verlag GTM No-110, 1986.
- [Lang3] Lang, S., *Elliptic Functions*. Springer Verlag GTM No-112. 1987.
- [Lang4] Lang, S., *Introduction to Modular forms*. Springer Verlag series of comprehensive studies in mathematics, 1976.
- [LayZ] Lay, G.J., Zimmer, G.H., "Constructing Elliptic Curves with Given Group Order over Large Finite Fields", LNCS, vol-877, Algorithmic Algebraic Number Theory. Springer Verlag, 1994.
- [LidN] Lidl, Niederreiter, H., *Finite Fields*, Theory and Applications, Cambridge University Press, 1991.
- [Men1] Menezes, A., *Elliptic Curve Cryptosystems*. Kluwer Academic Publications. 1994.
- [Men2] Menezes, A.(Ed), *Applications of Finite Fields*. Kluwer Academic Publications. 1994.
- [McEl] Mc Eliece, *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publications, 1992.
- [MOVW] Menezes, A., Onyszchuck, Vanstone, Wilson, "Optimal Normal Bases in  $GF(p^n)$ ", Discrete Applied Math. Vol-22, (1988/1989), 149-161.
- [More] Moreno, C., *Algebraic Curves Over Finite Fields*. Cambridge University Press, 1991.
- [Ono] Ono, T., *An Introduction to Algebraic Number Theory*, 1988.

- [POZe] Pohst, Zassenhaus, *Algorithmic Algebraic Number Theory*. Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1993.
- [Poll] Pollard, H., *The Theory of Algebraic Numbers*. Carus Monograph No-9 1961.
- [Rose] Rose, H.E., *A Course in Number Theory*. Oxford University Press, 1994.
- [Silv1] Silverman, J.H., *The Arithmetic of Elliptic Curves* Springer Verlag GTM No-106, 1986.
- [Silv2] Silverman, J.H., *Advanced Topics in The Arithmetic of Elliptic Curves*. Springer Verlag GTM No-151, 1994.
- [Shaf1] Shafarevich, I.R., *Number Theory I. Fundamental problems, Ideas and Theories*. Springer Verlag encyclopedia of mathematics series, 1995.
- [Shaf2] Shafarevich, I.R., *Number Theory II. Algebraic Number Theory*. Springer Verlag encyclopedia of mathematics series, 1991.
- [Weil] Weil, A., *Basic Number Theory*. Springer Verlag Universitext, 1978.